TASK ORDER

GST0013AJ0065

Reserve Component Automation (RCA)

in support of:

U.S. Army PEO EIS

Issued to:
CACI NSS, Inc.

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW
Washington, DC 20405

September 09, 2019
FEDSIM Project Number 12085ARM

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract.

C.1 BACKGROUND

C.1.1 PURPOSE

The purpose of this TO is to acquire performance-based information technology (IT) technical support services associated with Army projects, programs, applications, and infrastructure services in support of the Project Directorate (PD) Reserve Component Automation Systems (RCAS), the Army National Guard (ARNG) Distance Learning Project (DLP) programs and infrastructure services to support the PD RCAS, programs, and services to support the PD RCAS, and development, sustainment, and fielding of Information Management Architeture (IMA) projects, military IT infrastructure projects (ITII&R), programs, applications, architecture in support of the ARNG.

C.1.1.1 VISION

The PD RCAS vision is to enter into a working relationship with industry to accelerate the pace at which it develops and deploys critical software capabilities to the field, while providing innovative, efficient, and effective software development management processes. Additionally, PD RCAS is looking for innovative approaches to manage the sustainment of vital IT infrastructure for the Guard and Reserve components.

C.1.2 AGENCY MISSION

C.1.2.1 PD RCAS

PD RCAS is a Department of the Army (DA) organizational element within the Program Executive Office, Enterprise Information Systems (PEO EIS). PEO EIS provides infrastructure and information management systems to the Army enabling it to achieve its mission through comprehensive information ascendency. PEO EIS develops, acquires, and deploys tactical and management IT systems and products.

The PD RCAS is responsible for sustaining and modernizing automated information systems that enhance the Reserve Component's (RC) ability to achieve and sustain critical automation interoperability and accomplish unit mobilization planning, training, day-to-day operations, communications, and administration.

The PD RCAS also provides support to the total Army, to include the Active Component (AC), ARNG and United States Army Reserve (USAR) IT communities by providing support for business application and web support services. Specifically, PD RCAS supports the National Guard Bureau's software sustainment and DLP, the IT component of Military Construction (MILCON), and manages the USAR's RCAS production server enclave at Fort Bragg, NC.

C.1.2.2 ARNG DISTANCE LEARNING PROJECT (DLP)

The DLP is a congressionally mandated program designed to improve military readiness, enhance command, control, communications, and computers (C4), and practically serve America's communities by making available shared access to high-performance communications. DLP provides digital distance-learning-oriented classrooms to train soldiers, thereby increasing National Guard readiness, and promotes shared use to make classrooms available for use by the civilian community and allows Warfighters and their families to communicate between home station and deployed unit locations.

C.1.2.3 INFORMATION MANAGEMENT ARCHITECTURE (IMA)

The ARNG is an operational organization providing trained and deployment-ready Soldiers from the 54 States, United States (U.S.) Territories, and the District of Columbia (D.C.). The ARNG is fully capable of accomplishing state, national, and international missions during war and peace. To meet these requirements, the ARNG maintains a balanced mix of combat, combat support, and combat service support units. These units are structured to integrate seamlessly within active component units as needed, and are located in nearly 3,000 communities throughout the U.S., which enables them to respond rapidly to domestic emergencies.

The IMA Division is one of three divisions within the ARNG G6 organization of the ARNG Directorate, National Guard Bureau. The ARNG IMA Division is responsible for providing a broad range of IT services to the ARNG. The IMA Division includes branches responsible for Application Sustainment and Development, Data Center Operations, and Data Management.

C.1.2.4 IT INFRASTRUCTURE INTEGRATION AND REFRESH (ITII&R)

Military organizations (specifically: the Army Corps of Engineers, ARNG, USAR, and United States Marine Corps (USMC)) are currently responsible for the military construction requirements for the IT services for numerous sites throughout the U.S. A schedule of network implementation projects for the period of performance identified herein is not presently known; however, RCAS anticipates that it will continue to have responsibilities in this area.

C.2 SCOPE

The scope of this Task Order (TO) is to sustain system baselines, software applications and hardware functionality for Reserve Component Automation (RCA). The scope includes providing all labor, material, supplies, and services to sustain, deliver, test, and field applications and provide IT solutions consistent with PD RCAS, ARNG DLP, IMA, and ITII&R technical requirements.

C.3 CURRENT INFORMATION TECHNOLOGY (IT) ENVIRONMENT

C.3.1 RCAS

RCAS maintains the United States Army Reserve Command (USARC) operational environment, physically hosted and supported at the USARC Network Operations Center (NOC) at Fort Bragg, NC. The USARC NOC physically hosts and supports two, Level 2 Integrated Databases (IDBs). One IDB supports USAR units of the Major Subordinate Commands (MSC) located in the Continental United States (CONUS), while the other IDB supports the many units in the U.S. Army Civil Affairs and Psychological Operations Command (USACAPOC).

RCAS is a fielded Acquisition Category (ACAT) III Automated Information System (AIS) providing Army Reserve Components (RCs) with the capability to administer, manage, and more effectively mobilize forces in five primary functional areas:

- Mobilization
- Safety and Occupational Health
- Personnel Support
- Force Authorization
- Application Support / Back Office

The RCAS IDB is divided into four types of system architectures:

- ARNG Level 1
- ARNG Level 2
- USAR Level 1
- USAR Level 2

The technical specifications and topology between the ARNG and USAR IDBs are distinctly different due to the organizational attributes and force structure of each RC. The rationale for separate Level 1 and Level 2 instances is due to hierarchical reporting capabilities (i.e., report roll-up features) and a few applications are only used at the Component-level Headquarters.

The ARNG Level 1 IDB enables access to data for functional leaders at the ARNG Directorate and is physically hosted and supported at the ARNG Readiness Center in Arlington, VA. The Level 2 IDBs enable access to data for functional leaders and commanders at the State-level and is physically hosted and supported at each of the 54 Joint Force Headquarter (JFHQs).

The USAR Level 1 IDB enables access to data for functional leaders at the USARC and is physically hosted and supported at the USARC NOC at Fort Bragg, NC. The USARC NOC also physically hosts and supports two Level 2 IDBs. One IDB supports USAR units of the MSC located in the CONUS, while the other supports the many units within the USACAPOC.

There are two additional Level 2 IDBs that support outside CONUS (OCONUS) USAR units: one currently located in Germany for the 7th Civil Support Command (CSC) and the other in Hawaii for the 9th Mission Support Command.

RCAS, an enterprise information solution for the ARNG and the USAR, serves as a vital link between the Active and Reserve Components, and leverages data from authoritative sources and systems of record. The ARNG, at the Army Directorate of the National Guard Bureau (NGB) and the 54 States, U.S. Territories, and Washington, D.C. JFHQ, and the USAR, at the USARC headquarters and the various Command organizations, use the data in the many RCAS applications and its resulting records and reports to facilitate their missions. RCAS facilitates the accomplishment of hundreds of day-to-day administrative tasks at the unit level, thereby expediting the mobilization process. RCAS links approximately 4,000 ARNG and USAR sites worldwide that in turn support close to 10,500 units.

The RCAS suite of Applications consists of:

- Mobilization Planning Data Viewer (MPDV)
- Training and Operational Readiness Tracking (TORT)
- Deployment Manning Document (DMD)
- Battle Roster (BR)
- Tour of Duty (ToD)

The MPDV application has dramatically reduced the time and labor required to prepare and deploy soldiers through mobilization stations. General surveys of data-entry effectiveness show that, when utilizing MPDV, visibility unit readiness is significantly increased. Components of MPDV include:

- Safety Occupational and Health (SOH)
- Checklist Management Automated System (CMAS)
- Field Accident Table System (FATS)

Safety applications provide for the recording and reporting of aircraft and ground accidents as well as hazards. The lessons learned from this reporting helps to reduce the number of soldier accidents, thereby keeping soldiers ready for potential deployment. Components of safety applications include:

- Unit Personnel System/Command Management System (UPS/CMS)
- Military Personnel Office Orders (MILPO)
- Retirement Points Accounting Management (RPAM)
- Unsatisfactory Performance Letter (U-Letter)

The Personnel suite of applications addresses the unique needs of RC forces by managing orders and recording retirement points. Retirement point accounting currently supports only the Army National Guard. Components of the personnel msuite of applications include:

- Authorization and Requirements (A&R)
- Force Management (FM)
- Full Time Support (FTS)

- Mobilization Force File (MobFF)
- Organizational Authority (OA)
- Permanent Orders System (POS)
- RCAS Authorization Data for Personnel (RADPER)

Force Authorization applications allow users to develop strategic plans for current and future RC forces. Users are able to compare force management data, manage equipment requirements and distribution, compare authorization and requirements data, and create hypothetical scenarios. Components of force authorization applications include:

Application Support/Back Office

- RCAS Web
- RCAS Integrated Database (IDB)

RCAS Web is a web-based interface that provides users with a single point of access to all of the RCAS web-based applications. In addition, it provides system administrators with user account administration functionality, as well as organizational hierarchy creation and maintenance.

RCAS Applications	Acronym	Component
Mobilization Planning Viewer with	MPDV	ARNG & USAR
Training and Operational Readiness Tracking	TORT	
Deployment Manning Document	DMD	
Battle Roster	BR	
Tour of Duty	ToD	
Retirement Points Accounting Management	RPAM	ARNG
Unit Personnel System/Command Management System	UPS/CMS	
Military Personnel Office Orders	MilPO Orders	
Unsatisfactory Participation Letter	U-Letter	USAR
Full Time Support	FTS	USAR
Permanent Order System	POS	USAR
Mobilization Force File	MobFF	
Force Management/Organizational Authority	FM/OA	ARNG & USAR
Authorization & Requirements	A&R	
RCAS Authorization Data for Personnel	RADPer	
Safety and Occupational Health	SOH	ARNG & USAR
Checklist Management Automated System	CMAS	
Field Accident Table System	FATS	
RCAS WEB/Information Exchange Loader/Back Office	RCAS Web/BO	ARNG & USAR
RCAS Integrated Database	RCAS IDB	

The RCAS suite of applications recently completed a transition to a standard, architectural framework (i.e., Microsoft's .Net 4.0 MVC 3). Essential to PD RCAS' software process and product management roadmap is to build upon the standards established by leveraging automated tools and enabling RCAS to employ and optimize cloud technologies such as Platform-as-a-Service (PAAS) and/or Infrastructure-as-a-Service (IAAS), as appropriate.

The RCAS production environment takes advantage of virtual technology by using VMware 5.0, in which the applications are hosted on servers loaded with Windows Server 2008 R2 and Internet Information Server (IIS) 7.5. The data are stored on, and accessed from, a virtualized Database running Oracle version 11G R2. RCAS users access the software via client computers running the Army's Gold Master (AGM) image of Windows 7.

Each of the 54 ARNG JFHQs host the production environment described above. The USAR production environments are located at the Command Enterprise Data Center in Fort Bragg, NC, the 7th US Army CSC in Germany, and the 9th Mission Support Command in Hawaii.

C.3.2 ARNG DLP

DLP represents an evolving capability for the Government and served communities. Since classrooms were completed at different points within the continuing DLP deployment phase, a variety of hardware, software, desktops, and network packages were employed to support project objectives and interoperability requirements. 327 classrooms are brick and mortar, classrooms are fixed locations with the exception of periodic classroom relocation. Conversely, there are currently seven Mobile Distance Learning Classrooms (MDLC). The MDLC is a portable classroom developed with the intent to provide a learning environment that may be transferred among locations within a state or territory to bring the classroom to the soldier. All classrooms are connected via GuardNet. A typical learning environment has from 3 to 18 student workstations equipped with a computer, monitor, keyboard, microphone, and headphones and is networked via Ethernet Local Area Network (LAN). An average of 30 learning environment baselines are technically refreshed each calendar year; a learning environment baseline is defined as the minimally acceptable classroom technical learning environment. The contractor shall sustain learning environment baselines, classrooms, and functionality for RCAS and DLP.

DLP consists of 334 specially designed multimedia classrooms throughout the country, linked by a terrestrial network and satellite technologies. Changes to the Army's force structure have placed a heavy burden on the National Guard to retrain soldiers from one military specialty to another. In the past, such retraining required transporting soldiers to distant brick and mortar classrooms, an often costly and time-consuming process. The DLP gives significant opportunity to the Guard to maintain the required readiness while reducing overall training costs. The advantages of DLP to readiness include:

- An increase in the number of soldiers that can be trained simultaneously.
- A lower cost for instructors, student transportation, and physical plant.
- A reduction in the amount of time required to deliver requisite training to large, geographically dispersed groups.
- The ability to broaden the scope of education, making more information available to more people at the same time.

C.3.3 IMA

The IMA environment is a combination of legacy client-server and web-based applications described in Table 1.

Table 1 – IMA Core Enterprise Applications
Note: See accreditation status for applications identified below in Section J-Attachment AG

Application Description	Hardware Platform	Operating System	Other COTS Software
Automated Fund Control Orders System (AFCOS)/ JUMPS Standard Terminal Input System (JUSTIS) AFCOS performs the following: Order writing program for all types of duty orders for the ARNG; provides standardized format of orders; serves as a historical database for order register data; interface between orders and military pay for ease of creating payments to soldiers; interface between payrolls and fiscal accounting for input into Standard Financial System (STANFINS) and retention of historical accounting data; interface between personnel and financial systems for one-time entry; fund control program for Fund Managers to input and track reservations, obligations, and disbursements; provides automated files to Fiscal Accounting for creation of reservations; provides automated pre-validation of proper STANFINS data before passing to STANFINS; provides internal controls to prevent duplication of same periods for different duties; ensures use of proper fund manager codes by those having fund authority. JUMPS Standard Terminal Input System (JUSTIS) is a PAY SYSTEM input system.	HP Itanium DB And Web Servers	HP-UX 11.23	-Oracle 10 R2 -AccuCOBOL -Oracle Forms and Reports 9i
Acquisition Planning Board (APB) The APB application is a web-based application that Divisions to submit purchase requests to the APB for review and approval before the item or service can be acquired.	Intel-based DB And Web Servers	MS Windows Server 2000	-IIS 6.0 -SQL Server 2005 -SQL Server 2005 Reporting Services -Microsoft Visual Studio.NET 2005
Enterprise Data Warehouse (EDW) The ARNG EDW provides access to transactional data through a common querying and reporting interface and extends the Army Modernization Plan vision of “Winning the battlefield Information War," by providing reliable, high quality, and consistent data across all ARNG enterprise functional areas, suitable for analysis, forecasting, reporting, ad-hoc querying, and decision support processes. The EDW consist of seven data marts and one data provisioning capability: EDW Finance Data Mart EDW Real Property Data Mart EDW Environmental Data Mart EDW Equipment Reset Data Mart EDW Equal Opportunity Data Mart EDW Publications Data Mart EDW G1 Data Mart	HP Itanium App and DB Servers, and Windows App Server	HP-UX 11iv3and Windows Server 2003	-Cognos 10.1 BI Server -Oracle 11g

Application Description	Hardware Platform	Operating System	Other COTS Software
EDW Counterdrug Data Mart EDW SMS-A- data provisioning capability			
Geospatial Information System (GIS) GIS-NG provides geospatial information and services to the 54 Army National Guard (ARNG) States/Territories, Readiness Center, and the NGB Joint Programs Office. GIS-NG supplies data, software, and operating procedures to meet Federal and State mission requirements within the installations and environment business domain. GIS-NG is the focal point for access to geospatial information on ARNG installations. As such, GIS-NG feeds consistent and standardized (e.g., Special Data Standards for Facilities, Infrastructure, and Environment (SDSFIE) and Federal Geographic Data Committee (FGDC) geo-spatial information to other Army Mapper agencies.	HP ProLiant Blade Dell PowerEdge 2650 Dell PowerEdge 6650	MS Windows Enterprise Edition 2003	-MS SQL Server 2005 -ESRI ArcSDE v9.2 SP6 -ArcGIS desktop 9.3 SP2 - ArcGIS Server .NET frameworkversion 9.3 SP2 -Lizardtech Express Server 5.3 -ArcGIS desktop 10.0 SP2-ESRI license Manager (Flexlm) -GeoExpressfloating license manager
MyUnitPay (MUP) MyUnitPay is a web-based system utilizing an Oracle database. MyUnitPay provides the ARNG with the ability to pay soldiers at the unit level for Inactive Duty Training (IDT) pay, split training, Additional Flight Training Periods (AFTP's), Readiness Management Period (RMP), Special Duty Assignment Pay (SDAP), Foreign Language Proficiency Pay (FLPP), Funeral Honors, and short tour Active duty pay certification. MUP was developed as a replacement for the IDT portion of the AFCOS Request For Orders / Inactive Duty (RFO/IDT).	HP Itanium DB Server; HP BL460c Blade Server (4 CPU's 4GB MEMORY)	HP-UX 11.23; ESX VMWARE 4.1 Update 2 running Windows 2003 Server Standard Edition	-Oracle 10 R2 -AccuCOBOL -Crystal Reports 10 -Adobe Acrobat Professional 6
Standard Installation/Division Personnel System (SIDPERS) SIDPERS-ARNG is a management information system designed to support the functional areas of strength accounting, personnel management, information retrieval, and external interfaces at the field operating level. Integrated Pay and Personnel System Army (IPPS-A) is scheduled to subsume SIDPERS functionality in 2014.	HP Itanium DB and Web Servers	HP-UX 11.23	-Oracle 10 g R2 -Oracle Forms and Reports 9i
Total Army Personnel Database – Guard (TAPDB-G) TAPDB-G provides a variety of personnel data in support of the Headquarters Operating Level personnel management activities at the National Guard Bureau. Currently, SIDPERS supports personnel management activities at the individual state level.	IBM Mainframe	Z/OS	-DATACOM-DB -COBOL -DataQuery -TSO -ROSCOE

Application Description	Hardware Platform	Operating System	Other COTS Software
Web Corporate Management System (WebCMS2) WebCMS is a web-based corporate management tool for management of the United States Army Operational Support Airlift Command's (OSACOM) assets. WebCMS allows the users to enter fuel and maintenance expense tickets and maintain aircraft data and personnel information. WebCMS allows for the reconciliation of budget data with the Defense Cash Accountability System (DCAS). OSACOM personnel are required to use WebCMS for posting data and for immediate access to current information on OSACOM units, Points of Contact (POC), aircraft, fuel, and other purchases (ticket and ticket items), telephone rosters, unit Department of Defense Activity Address Codes (DODAACs), budget, aircraft assignment history, aircraft missions, aircraft and personnel flight hours and selected personnel data. Existing system is on COOLGEN v6.5. Contractor shall migrate to .NET	Intel-based DB and Web Servers	MS Windows Server 2003 SP1	-IIS 7.0 -SQL Server 2005 -CA Gen 6.5 -ASP -MS Visual Studio -Adobe Studio -Crystal Reports 8.5

C.3.4 ITII&R

Military organizations (specifically the Army Corps of Engineers, ARNG, USAR, and USMC) have relied on PD RCAS to oversee and manage the efforts in the design and installation of network IT projects since November 2009; primarily PD RCAS supports the IT network implementation work for Military Construction (MILCON) activities. PD RCAS anticipates an average of 15 IT infrastructure-related projects per calendar year.

C.4 OBJECTIVE

RCAS
Historically, RCAS sustainment has experienced challenges due to the interactions and dependencies between the applications and the integrated database. PD RCAS anticipates innovative solutions to deliver quality software in a timely, effective, and cost-effective manner.

DLP
Sustain ARNG DLP and ensure the designs meet or exceed functional and operational requirements, which include improved readiness, C4 capabilities, and shared-usage of facilities.

IMA
Consolidate applications as part of an overall effort to leverage a secure common operating environment. The application sustainment activities will include focus on incrementally modernizing the technology to leverage virtualization, multi-tiered architectures in a secure Demilitarized Zone (DMZ). See Section J-Attachment P for IMA Software Development Lifecycle.

ITII&R
Design, procure, install, and test local network infrastructures.

C.5 TASKS

Task 1 – Transition (Mixed)
- Subtask 1 – Transition In (CPAF)
- Subtask 2 – Transition Out (FFP)

Task 2 – Program Management (FFP)
- Subtask 1 – Accounting for TO Services
- Subtask 2 – Coordinate a Program kickoff meeting
- Subtask 3 – Prepare an Integrated Program Management Review (IPMR)
- Subtask 4 – Prepare and update the Program Management Plan (PMP)
- Subtask 5 – Earned Value Management (EVM) Criteria
- Subtask 6 – After Action Reports (AAR)

Task 3 – RCAS Core Sustainment (CPAF)
- Subtask 1 – Planning and Implementation of Software
- Subtask 2 – RCAS Software
- Subtask 3 – Systems Analysis and Systems Architecture
- Subtask 4 – Integrated Data Environment (IDE)
- Subtask 5 – Databases
- Subtask 6 – Information Exchanges (IE)
- Subtask 7 – Quality Assurance
- Subtask 8 – Configuration Management (CM)
- Subtask 9 – Product Testing
- Subtask 10 – Government Secure Test Environment (STE)
- Subtask 11 – Software Deployment Management
- Subtask 12 – Information Assurance (IA)
- Subtask 13 – Requirements Management
- Subtask 14 – Asset Management
- Subtask 15 – Enterprise Training and Documentation

Task 4 – RCAS Support (FFP)
- Subtask 1 – Enterprise Service Desk
- Subtask 2 – Field Support
- Subtask 3 – USARC Operations
- Subtask 4 – USARC COOP Support
- Subtask 5 – Training Server Enclave
- Subtask 6 – Special Project Support
- Subtask 7 – Conduct Training

Task 5 – Contractor Environment (FFP)
- Subtask 1 – Establish Development and Integration Environment

Subtask 2 – Office Automation
Subtask 3 – Asset Management

Task 6 – Hardware and Software Products (FFP)
Subtask 1 – Purchasing
Subtask 2 – Product Assembly and Shipment
Subtask 3 – Product Installation

Task 7 – IT Infrastructure Integration and Refresh (Mixed)
Subtask 1 – Planning and Design (P&D) (CPAF)
Subtask 2 – Network Installation (FFP)

Task 8 – DLP Core Sustainment (CPAF)
Subtask 1 – Help Desk
Subtask 2 – Sustaining Engineers
Subtask 3 – Equipment Maintenance
Subtask 4 – Enterprise Support

Task 9 – IMA Core Sustainment (CPAF)
Subtask 1 – Planning and Implementation of Software
Subtask 2 – Establish Development Environment
Subtask 3 – Sustainment Support
Subtask 4 – System Analysis
Subtask 5 – IMA Core Sustainment
Subtask 6 – Software Deployment Management
Subtask 7 – Configuration Management (CM)
Subtask 8 – Testing
Subtask 9 – Government Secure Testing and Integration Environment (STIE)
Subtask 10 – IA Security, Risk Remediation and Mitigation
Subtask 11 – Legacy COTS/GOTS Software
Subtask 12 – Asset Management
Subtask 13 – Enterprise Service Desk
Subtask 14 – Information Assurance Requirements
Subtask 15 – Conduct Training

Task 10 – Surge/Special Projects (CPAF)

C.5.1 TASK 1 – TRANSITION

C.5.1.1 SUBTASK 1 – TRANSITION-IN

The contractor shall prepare a Transition-In Plan update for inclusion in the Integrated Program Management Review (IPMR), until such time as all tasks have been transitioned over to this TO (see Section F, Deliverable #1). Transition ensures the Contractor is afforded the opportunity to develop a thorough understanding of the legacy system life-cycle management processes and

system requirements; define, implement, and receive Government concurrence of any new or changed management processes based on the contractor's proposal, and assume responsibility for system sustainment.

The emphasis of the transition is to minimize disruption of service to applicable Government legacy systems. The Government encourages a collaborative relationship with the contractor and encourages incorporating new, efficient, and innovative approaches to meeting the requirements in this TO. The contractor's Transition-In Plan shall identify the time period for its project team to receive sufficient levels of enterprise training and familiarization to clearly understand all aspects of the project and accept full responsibility for the current systems and daily operations. During this transition period, the incumbent contractor has been tasked by the Government to support the knowledge transfer to the succeeding contractor. The incumbent contractor is responsible for all system sustainment activities until the transfer of responsibilities is finalized to the Government's satisfaction.

Knowledge transfer shall address, at a minimum:

a. System technical and functional/operational descriptions
b. System functional and technical capabilities
c. System engineering and design
d. System security features and system specific Defense Information Assurance Certification and Accreditation Process (DIACAP) status
e. Identification of all known risks

The Contractor shall complete transition-in by September 13, 2013.

The transition shall ensure minimum disruption to vital Government operations. The contractor shall ensure that there is no transition-related service degradation during transition in.

The final Transition-In Plan is due no later than (NLT) five workdays after TO start. The contractor's final Transition-In Plan shall include, at a minimum, the following:

a. An overview of the transition effort
b. A schedule with milestones and tasks
c. Description of activities to transition
d. Plan for transition of Government-Furnished Information (GFI)/Government-Furnished Equipment (GFE)
e. Plan to transition knowledge and information from incumbent contractor Key Personnel
f. Identification of potential risk or problem areas and remediation plan

C.5.1.2 SUBTASK 2 - TRANSITION OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor and Government personnel at the expiration of the TO. The contractor shall provide a Transition-Out Plan NLT 90 days prior to expiration of the base Period of Performance (PoP) and update the plan NLT 90 prior to expiration of each exercised option period (see Section F, Deliverable #2). The contractor shall identify how it will

coordinate with the incoming contractor and Government personnel to transfer knowledge regarding the following:

a. Program management processes
b. Points of contact
c. Location of technical and program management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor-to-contractor coordination to ensure a seamless transition.
f. Transition of Key Personnel
g. Identify schedules and milestones
h. Identify actions required of the Government

The contractor shall establish and maintain effective communication with the incoming contractor and Government personnel for the period of the transition via weekly status meetings.

Upon delivery of the final version release or other deliverable under this TO, the Contractor shall deliver to the Contracting Officer's Representative (COR), the following:

a. All framework, source code (fully compliable package), libraries, database tables, scripts, resources, modules, and all other related materials on the Government system and all software code.
b. All procedures to move modules to test/production environments, maintenance procedures, reference materials, technical documentation, user manuals, training and/or classroom materials, and all other related documentation.
c. Documentation to include system architecture diagrams, configuration management procedures (to include creating new modules, modifying code, testing, checking in and out modules, production releases, version control, etc.), system administrator procedures, database structure documentation, and data dictionary.

C.5.2 TASK 2 – PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this TO. The contractor shall effectively and efficiently manage project cost, schedule, and performance utilizing integrated program management processes across all aspects of the TO tasks and activities. The Contractor shall use innovative approaches to strategic technical planning as well as solutions to overcome operational challenges and obstacles.

The Contractor shall further provide human resources management, data/deliverable management, risk management, configuration control, test and evaluation management, conduct engineering work group (EWG) meetings, and monitor Information Assurance (IA) activities and impacts. Work products produced as part of this activity include producing weekly Joint Status Reviews (JSR), monthly and as-required Contract Discrepancy Report Lists (CDRLs), reports, deliverables, and program management and financial reviews.

The Government will utilize an Award Fee Determination Plan (AFDP) to monitor and incentivize CPAF Tasks (see Section J, Attachment J). The Government will utilize a Quality Assurance Surveillance Plan (QASP) to monitor FFP Tasks (see Section J, Attachment L).

C.5.2.1 SUBTASK 1 – ACCOUNTING FOR CONTRACT SERVICES

The Office of the Assistant Secretary of the Army (Manpower & Reserve Affairs) operates and maintains a secure Army data collections site where the contractor shall report ALL contractor manpower (including subcontractor manpower) required for performance of this contract. The contractor is required to completely fill in all the information in the format using the following web address: https://cmra.army.mil

The required information includes:

a. Contracting Office, CO, COR.
b. Contract number, including Task and Delivery Order number.
c. Beginning and ending dates covered by reporting period.
d. Contractor name, address, phone number, and e-mail address, and identity of contractor employee entering data.
e. Estimated direct labor hours (including subcontractors).
f. Estimated direct labor dollars paid this reporting period (including subcontractors).
g. Total payments (including subcontractors).
h. Predominant Federal Service Code (FSC) reflecting services provided by the contractor (separate predominant FSC for each subcontractor if different).
i. Estimated data collection costs.
j. Organizational title associated with the Unit Identification Code (UIC) for the Army Requiring Activity (the Army requiring Activity is responsible for providing the contractor with its UIC for the purposes of reporting this information.
k. Locations where contractor and subcontractor perform the work (specified by zip code in the United States (U.S.) and nearest city and country (when in overseas locations) using standardized nomenclature on website).
l. Presence of deployment or contingency contract language.
m. Number of contractor and subcontractor employees deployed in theater this reporting period (by country).

As part of its submission (see Section F, Deliverable #3), the contractor shall also provide the estimated total cost (if any) incurred to comply with this reporting requirement. Reporting period will be the period of performance, NTE 12 months, ending September 30 of each Government fiscal year and must be reported by October 31 of each calendar year or at the end of the contract, whichever comes first. Contractors may use Extensible Markup Language (XML) data transfer to the database server or fill in the fields on the website. The XML direct transfer is a format for transferring files from a contractor's systems to the secure web site without the need for separate data entries for each required data element at the website. The specific formats for the XML direct transfer may be downloaded from the web.

C.5.2.2 SUBTASK 2 – COORDINATE A PROGRAM KICKOFF MEETING

The contractor shall schedule and coordinate a Program Kick-Off Meeting at a location approved by the Government. The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include contractor Key Personnel, representatives from the directorates, other vital Government personnel, and the Federal Systems Integration and Management Center (FEDSIM) COR. The contractor shall provide the following at the Kick-Off Meeting:

a. Transition In-Plan – Final (see Section F, Deliverable #1)
b. Program Management Plan (PMP) initial draft (see Section F, Deliverable #4)
c. Software Development Plan (SDP) (see Section F, Deliverable #5)
d. Earned Value Management (EVM) Plan (see Section F, Deliverable #6)
e. Quality Control Plan (QCP) (see Section F, Deliverable #7)

C.5.2.3 SUBTASK 3 – PREPARE AN INTEGRATED PROGRAM MANAGEMENT REVIEW (IPMR)

The contractor's Program Manager (PM) shall develop and deliver an Integrated Program Management Review (IPMR) (see Section F, Deliverable #8) monthly using Microsoft Office Suite applications via electronic mail to the Technical Point of Contact (TPOC) and the COR. The IPMR shall include the following:

a. Activities during reporting period, by task (Include: On-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
b. Risk and issue tracking to include mitigation plans and strategies, and corrective actions
c. Staffing Plan that includes initial filling of billets as well as ongoing contingencies to handle personnel turnover and areas of shortfall.
d. Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
e. Summary of trips taken
f. EVM statistics as per TO Section C.5.2.5.
g. Cost for each CLIN for the current month and TO year to date.
h. Projected cost of each CLIN for the upcoming month.
i. Cost and schedule comparison data / monthly performance reports.
j. Metrics on problem areas such as trouble tickets and system problem reports, whether identified by the Government or the contractor. Metrics on problem areas shall include a trend analysis.
k. Integrated Baseline Review (IBR) within 90 days of project start and 30 days prior to end of base and each option year (see section F, deliverable #9).
l. 90 days prior to end of base and each option year include socioeconomic subcontracting plan compared to actual performance.

C.5.2.4 SUBTASK 4 – PREPARE AND UPDATE A PROGRAM MANAGEMENT PLAN (PMP)

The contractor shall develop and deliver a Draft and Final Program Management Plan (PMP) that is based on the contractor's proposed solution (see Section F, Deliverables #4). Upon Government approval, the Contractor shall execute the PMP. The PMP is an evolutionary document, and as such, the contractor shall provide PMP updates throughout the TO performance period as changes in management items occur. The contractor shall update all appropriate sections of the PMP that are affected by these changes.

At all times, the contractor shall operate under a Government-approved PMP.

The contractor shall document all support requirements in the PMP. The PMP shall describe the contractor's organization, resources, processes, and management controls that will be employed. The PMP shall include a staffing plan. The PMP shall define the proposed organizational structure (including responsibilities and reporting structure), how personnel will be assigned throughout the contractual period, and how the proposed project team will interface with both the contractor's corporate structure and the Government command structure. The PMP shall also address how the contractor contributes to achieving socio-economic business opportunity targets. The PMP shall include the contractor's management process, subcontractor management process, external contractor communication plan (for integrating IT tasks outside the scope of this TO), and communication plan with the Government. The PMP shall detail the contractor's Standard Operating Procedures (SOPs) for all operational and developmental tasks. The PMP shall define policies and procedures for managing and directing the effort for productivity, quality, cost control, and early identification of risks and resolution of issues. The PMP shall include the comprehensive project schedule. The PMP shall provide for a Work Breakdown Structure (WBS), as per data item description DI-MGMT-81334B, and associated responsibilities and partnerships between Government organizations by which the contractor shall manage all work. The PMP shall include the contractor's Software Development Plan (SDP) and EVM Plan.

C.5.2.5 SUBTASK 5 - EARNED VALUE MANAGEMENT (EVM) CRITERIA

The Contractor shall employ EVM in the management of this TO. While the Government reserves the right of final approval, a joint determination will be made by the Government and contractor as to where EVM will be applicable. Generally, the Government will not require EVM to be applied against level of effort (LOE) tasks or firm-fixed price (FFP) activities. The contractor's system shall meet the guidelines and be maintained in accordance with the requirements for EVMS as described in this TO, under Defense Federal Acquisition Regulation Supplement (DFARS) Clauses 252.234-7001 and 7002 . The IPMR (see Section F, Deliverable #8) shall be developed, maintained, updated, and reported on a monthly basis. Reports shall conform to Data Item Description (DID) Number DI-MGMT-81861. The qualities and operating characteristics of earned value management systems are described in American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard-748, Earned Value Management Systems. A copy of the standard is available from Global Engineering

Documents (1-800-854-7179) and will explain all variances greater than 10%, based on work accomplished as of the date of the report and whether the performance goals will be achieved, and discuss the corrective actions that will be taken to correct the variances and the risk associated with the actions. Reports may be tailored to meet operational requirements upon approval by the Government.

C.5.2.6 SUBTASK 6 - PREPARE AFTER ACTION REPORTS (AAR)

The Government will identify the need for After Action Reports (AAR) when a request for travel is submitted or after participating in a meeting, discussion, conference, seminar, training, event, etc. The contractor shall retain a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, lodging costs, transportation costs, Meals, Incidentals and Expenses (MI&E) costs, Other costs (describe costs identified as other costs) and POC at travel location (see Section F, Deliverable #10).

C.5.3 TASK 3 – RCAS CORE SUSTAINMENT (CPAF)

The contractor shall acquire and maintain an in-depth understanding of the overall system architecture, system design, and functionality requirements to include system of systems interfaces. The contractor shall sustain system baselines and software applications for RCAS, ensuring timely security and product updates and quality releases. The contractor shall sustain the hardware functionality for the USAR RCAS systems at USARC. The contractor shall be responsible for cost control, adherence to mutually agreed upon schedules, and technical quality of work.

The contractor shall provide system development and maintenance in support of the Army RCs. Commercial products and processes shall be used to the greatest extent practicable. The contractor shall provide system sustainment services for software applications, database applications, and other solutions, to include all the associated activities required to enhance, integrate, implement, and maintain the RCAS solution.

C.5.3.1 SUBTASK 1 – PLANNING AND IMPLEMENTATION OF SOFTWARE

C.5.3.1.1 The contractor shall define a software approach appropriate for the computer software development effort to be performed under this TO. This approach shall be documented in the contractor's SDP (see Section F, Deliverable #5). The contractor shall adhere to the Government-approved SDP for all software to be developed and maintained.

C.5.3.1.2 The SDP shall define the contractor's proposed lifecycle model and the processes used as a part of that model. For the purposes of this TO, the term *lifecycle model* is defined in Institute of Electrical and Electronics Engineers/ Electronic Industries Alliance (IEEE/EIA) Std. 12207-2008. The SDP shall describe the overall lifecycle and shall include primary, supporting, and organizational processes based on the work content of this solicitation. In accordance with the framework defined in IEEE/EIA Std. 12207-2008, the SDP shall define the processes, the activities to be performed as a part of the processes, the tasks that support the activities, and the

techniques and tools to be used to perform the tasks. The SDP shall maximize the use of automated tools and industry best practices (e.g., test-driven development and integrated quality processes). The SDP shall include and leverage the automated tools PD RCAS has made investments in and mandated by higher headquarters. Because IEEE/EIA Std. 12207-2008 does not prescribe how to accomplish the task, the Contractor shall describe its approach in sufficient detail within the SDP in order that the Government may assess whether the contractor's approach is viable (see Section J, Attachment O (RCAS Baseline)).

C.5.3.1.3 The SDP shall contain the information defined by ISO/IEC/IEEE 15289:2011, section 7.3 (generic content) and 10.21 Development plan In all cases, the level of detail shall be sufficient to define all software development processes that clearly demonstrate integration of quality assurance best practices throughout the software development lifecycle, activities, and tasks. Information provided shall include, at a minimum, specific standards, methods, tools, Commercial Off-the-Shelf (COTS)/Government Off-the-Shelf (GOTS), actions, strategies, and responsibilities associated with development and testing.

C.5.3.1.4 Additionally, the SDP shall describe an integration and training plan focused on providing the Government a thorough understanding of the Contractor's software development methodologies and testing tools and processes. This training plan shall begin with a detailed introduction during the Transition-In period and be continue throughout the entire period of performance.

C.5.3.1.5 The contractor shall:

a. Define an innovative and efficient lifecycle software support methodology/approach consistent with total system requirements.
b. Provide support characteristics that are managed as an integral part of system development.
c. Provide system lifecycle support and sustainment.

C.5.3.1.6 The contractor shall incorporate innovative holistic solutions within a rapid development and synergistic deployment approach for quality software within a flexible and mission responsive and adaptive methodology.

C.5.3.1.7 Software development processes and resultant deliverables under this TO shall be a series of rapid developments that deliver incremental capabilities in shortened timeframes as defined in roadmaps developed and delivered by the contractor. The contractor shall employ continuous integration best practices in developing software solutions.

C.5.3.1.8 Based on a plan for each project, the contractor shall complete and deliver a version-controlled software release for fielding. Most projects will require several iterations culminating in an update to the field. The scope of every project will be tailored based upon the projected level of effort, driving longer or shorter iterations and update schedules as required.

C.5.3.1.9 The contractor shall lead technology planning to evaluate the IT marketplace, its trends and growth to develop periodic technology refresh and enhancement plans. The

contractor shall maintain a list of business requirements and the corresponding roadmaps.

C.5.3.1.10 The contractor shall provide technical/management leadership of analysis of highly specialized applications and operational environments, functional systems analysis, design, integration, documentation, and implementation of technical solutions.

C.5.3.2 SUBTASK 2 –RCAS SOFTWARE

C.5.3.2.1 The contractor shall reduce the requirements backlog of approximately 200 by 15% per annum while maintaining an operational tempo (OPTEMPO) for the prioritized requirements defined by the Requirements Control Board (RCB) and any System Problem Reports (SPRs) no later than three months after TO start.

C.5.3.2.2 The contractor shall develop and sustain the RCAS Developed Applications Software Baseline. To support this activity, the contractor shall evaluate the current enterprise Business Process Model (BPM) and make recommendations for improvement. The BPM (see Section F, Deliverable #11) shall be broken down by discrete areas (i.e., Applications, Database, and Information Exchanges), as well as at the enterprise level.

C.5.3.2.3 The contractor shall use industry best practices for secure software design and development methodologies to ensure that applications placed into a production environment have no Category I and II security vulnerabilities.

C.5.3.2.4 The contractor shall maintain existing business functionality and shall be required to develop functional enhancements to existing software as approved by the Requirements Control Board (RCB). The contractor shall employ mature software development and sustainment processes.

C.5.3.2.5 The contractor shall implement industry-standard software lifecycle management processes that support and direct multiple development teams working in parallel and in collaboration with the user community to accomplish development efforts using an iterative-development approach.

C.5.3.3 SUBTASK 3 – SYSTEMS ANALYSIS AND SYSTEMS ARCHITECTURE

C.5.3.3.1 The contractor shall conduct analyses and identify technologies to enhance the RCAS suite of applications, capitalizing on advancements in software development, automated testing, release methodologies, managing external interfaces, software security, mobile computing, data storage, and hosting environment. For each analysis the contractor shall utilize the following criteria: availability, maintainability, expandability, reliability, and conformance to Federal functional, security, and budgetary requirements.

The contractor shall identify resources required to implement each recommendation. As directed by the Government, the contractor shall deliver a system analysis with recommendation as described below.

C.5.3.3.1.1 Approved recommendations shall require further analysis. Analysis shall include the following elements:

a. Functional/technical requirements
b. The impact on relevant internal/external system(s)
c. Courses of Action (COA) based on current industry accepted methodologies coupled with innovative solutions
d. Results and findings, providing recommendations on systems integration and standardization
e. Implementation plans
f. Real-time Integrated Data Environment for Government review and feedback for software development projects

C.5.3.3.2 The contractor shall gather and review existing documentation and conduct interviews with key RCAS personnel to gain a thorough understanding of the RCAS environment. Within three months of TO award, the Contractor shall deliver a holistic review of the RCAS architecture and design. The assessment deliverable (see Section F, Deliverable #12) shall include the following:

- Analysis of the existing operational state of the production environment to determine overall stability and reliability and identify vulnerabilities.
- A detailed review of the system software, its strength and weakness, conformance to Microsoft .NET 4.0 MVC 3 standards, and an overview of the reliability, security, availability, and portability.
- The following standard DOD Architectural Framework (DODAF) views and update biennially
    - AV-1 Overview and Summary Information
    - AV-2 Integrated Dictionary
    - OV-1 High Level Operational Concept Graphic
    - OV-2 Operational Node Connectivity Description
    - OV-3 Operational Information Exchange Matrix
    - OV-5 Operational Activity Model
    - SV-1 System/Services Interface Description
    - SdtV-1 Technical Standards Profile
- Identify deficiencies and necessary steps for RCAS to comply with the DODAF. Conformance is achieved when:
    - The data is defined according to the DODAF Meta-model (DM2) concepts, associations, and attributes.
    - The architectural data is capable of transfer in accordance with the Physical Exchange Specification (PES).
- A roadmap for automating existing and future Information Exchanges (IEs) leveraging as much as possible the existing tool set (i.e., Oracle Date Integrator).
- A roadmap for complying with the Directive-Type Memorandum (DTM) 2007-015 USD(P&R) – "DOD Social Security Number (SSN) Reduction Plan"

C.5.3.3.3 Within 12 months of TO award, the contractor shall deliver a plan to take advantage of initiatives such as Platform-as-a-Service (PAAS) or Infrastructure-as-a-Service (IAAS) that are compatible with an approved Department of Defense (DOD)/Army hosting environment (see Section F, Deliverable #13). The contractor shall define an incremental approach to achieving the required capability and perform the following:

C.5.3.3.3.1 Analysis

a. The contractor shall perform analysis of the current solution for the applications, technology, and production environment (see section F, deliverable #14).
b. The contractor shall observe, capture, and evaluate current performance and provide recommendations for improvement.
c. The contractor shall verify the Government's operating environment specifications and identify any risks or technology impacts of the Government's specification.
d. The contractor shall establish baseline capacity and performance metrics for benchmarking purposes.
e. The contractor shall identify all factors that can inhibit an application interface from being automated without application modification.

C.5.3.3.3.2 Design

a. The contractor shall deliver a detailed Systems Architecture (see Section F, Deliverable #15) for the proposed solution. The Systems Architecture shall include:
    1. Generalized schematics.
    2. Design and solution strategy.
    3. Process specification.
    4. IA, disaster recovery, and business continuity capabilities.

b. The contractor shall deliver a Detailed Design which shall specify (see Section F, Deliverable #16):
    1. Interface specification.
    2. Schematics.
    3. Detailed process flows.
    4. Detailed configurations specifications.

c. The contractor shall deliver a migration strategy (see Section F, Deliverable #17).

d. The contractor shall deliver a Test Strategy considering (see Section F, Deliverable #18):
    1. Integration testing.
    2. Migration testing.
    3. Regression testing.
    4. Performance testing.
    5. IA and disaster recovery.

C.5.3.3.3.3 Build /Develop

a. The contractor shall develop and deliver Test Plans and Test Cases for (see Section F, Deliverable #19):
    1. Integration testing.
    2. Migration testing.
    3. Regression testing.
    4. Performance testing.
    5. IA and disaster recovery.

C.5.3.3.4 The contractor shall operate and maintain RCAS's systems architecture to meet the objectives and requirements of the project directorate by requiring an integrated set of activities and supporting documents that will execute RCAS's strategic vision, program concepts, communication plans, and implementation strategies while reducing lifecycle costs.

C.5.3.3.4.1 The contractor shall sustain systems engineering processes by providing a methodology that incorporates change planning/management, requirements gathering, and development of standardized, repeatable processes, roadmaps, and implementation plans. The Contractor shall develop and document appropriate processes and procedures for implementation across the program (see Section F, Deliverable #20):

C.5.3.3.4.2 The contractor shall ensure that any future IT architecture is sufficiently sized, maintained, and robust enough to support the timely execution of workload. When implementing hardware, software, and network upgrades, the contractor shall ensure integration and compatibility with the most current Army architectural directives.

C.5.3.3.4.3 The contractor shall provide continuous leadership, innovation, monitoring, control, and management of engineering changes and provide a forum to facilitate and encourage collaboration between key stakeholders.

C.5.3.3.4.4 The contractor shall focus on the optimizing productivity and product quality while reducing the occurrence of inefficient systems and processes through an integrated systems engineering approach that utilizes industry best practices. Design concepts shall include provisions for technology refreshes that will capitalize upon emerging technological advances available in COTS product offerings.

C.5.3.3.4.5 The contactor shall inform and advise the Government on cross-cutting architecture and technical issues that may impact the enterprise.

C.5.3.3.4.6 The contractor shall ensure existing and future hardware/software solutions comply with all Federal, DOD, and Army architecture and IA and security standards.

C.5.3.3.4.7 The contractor shall support the Government's Requirements Control Board (RCB) processes. Support includes providing technical briefings relating to RCAS projects as needed in preparation for, and in support of, quarterly RCB meetings.

C.5.3.4 SUBTASK 4 – INTEGRATED DATA ENVIRONMENT (IDE)

C.5.3.4.1 The contractor shall establish and maintain a secure IDE that includes a real-time, collaborative environment that enables access to the contractor's software development environment, providing authorized government stakeholders with on-demand on-line access to work products under development commencing at the start of work. The purpose of the IDE is to create a seamless, collaborative data environment for the contractor and Government team that contains all pertinent data about the project throughout its development and delivery.

C.5.3.4.2 The IDE shall host all data referenced or produced in support of this TO, including cost, schedule, and technical data and deliverables. This data management program, including IDE structure, format, processes, and procedures, shall be documented within the PMP. At a minimum, the IDE shall contain the following information:

a. Current IPMR
b. All past IPMRs
c. Current Transition Plan
d. SDP
e. Current EVM Plan
f. Current and Past EVM Statistics
g. Current PMP
h. All After Action Reports
i. Asset Management Inventory
j. Status of deliverables (pending delivery, delivered pending Government acceptance, or Government accepted)
k. Current and past period cost data by CLIN (e.g., Labor, Travel, Tools, ODCs)
l. Detailed results of Quality Assurance (QA) audits
m. Labor time accounting, in accordance with prime contractor's approved accounting system.

C.5.3.4.3 The Contractor shall recommend additional data items not specified in Section F, Deliverables, in support of the processes/procedures that the Contractor will use to satisfy the requirements of the TO.

C.5.3.4.4 Data shall be protected in accordance with the appropriate Program Protection Plans IA guidelines. The Government reserves the right to observe all contractor efforts to accomplish the TO requirements and reserves the right to provide feedback as regards to contractor processes.

C.5.3.5 DATABASES

The contractor shall administer databases and incorporate changes, or updates, to the supporting data models, schemas, data dictionary and related support software. The contractor shall provide continuous improvement in the integration of the information within the database to facilitate data sharing across the applications. The contractor shall remain cognizant of Government data

standards in order to ensure full compliance with Government data standards (see http://staging.bizhelper.com/Army-Information-Architecture-Document-3.0-content/appendix-e-catalog-of-data-standards.html as an example)

C.5.3.6 SUBTASK 6 – INFORMATION EXCHANGES (IE)

The contractor shall automate, to the greatest extent possible, all IEs through the use of Oracle Data Integrator (ODI) and other solutions. The contractor shall analyze, coordinate, and develop technical solutions, defined by the requirements, for all IEs (see Section F, Deliverable #21). The contractor shall assist the Government in monitoring changes to and sustainment of the existing IEs. The contractor shall maintain technical specifications, and incorporate changes, or updates to the software and documentation as required, but at a minimum, on an annual basis.

C.5.3.7 SUBTASK 7 – QUALITY ASSURANCE

C.5.3.7.1 GENERAL

The contractor shall plan, develop, document, and implement a Software Quality Assurance (SQA) Program to be defined in the Software Quality Assurance Plan (SQAP) (see Section F, Deliverable #22) to ensure that comprehensive software quality is attained and all contractual requirements are satisfied. The contractor‘s SQA Program shall adhere to International Organization for Standardization (ISO) requirements, or other industry-recognized standards. The contractor’s SQA Program shall be applied to the following: software requirements; software design; software engineering standards, practices, and procedures; computer program implementation; software documentation, software testing; software library controls; configuration management; corrective action; and subcontractor administration.

C.5.3.7.2 MANAGEMENT

Effective SQA management shall have sufficient, well-defined responsibility, authority, and the organizational freedom to identify and evaluate quality problems and to initiate, recommend, and/or provide solutions. The contractor shall regularly review the adequacy of the SQA Program and revise and adjust the Program to ensure that the TO quality standards are satisfied. The term ―*SQA Program Requirements* are used herein includes the collective requirements of the standard.

C.5.3.7.3 REPORTING

The Contractor shall ensure objective evaluations and reports on software quality are delivered.

C.5.3.7.3.1 Results of all SQA activities shall be documented in industry best practice formats and shall be delivered to the FEDSIM COR and RCAS TPOC. Failure on behalf of the contractor to promptly report discovered discrepancies may be considered non-compliance with TO requirements.

C.5.3.7.4 INSPECTION AND ACCEPTANCE

C.5.3.7.4.1 QUALITY CONTROL (QC)

The contractor shall incorporate an effective quality control program throughout the SDP to ensure services are performed in accordance with this TO. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services.

The contractor shall ensure that the technology products, services, and solutions it provides are of high quality, are fully integrated with the RCAS production environment, and are tested to include hardware, software, security, operating systems, and networks.

C.5.3.7.4.2 MEASUREMENTS

The contractor's performance shall be measured by Service Level Agreements (SLA) (e.g., IA compliance, performance, features, repeatability, backward compatibility, seamless release with minimal impacts to existing application functionality, trouble ticket responsiveness and resolution to end users, and System Problem Reports (SPRs) generated during testing). Other areas of non-SLA evaluation include: meeting end user requirements/expectations, meeting regulatory and statutory requirements, end user involvement throughout the development process, ease of use/usability, portability, and innovation.

The contractor shall provide QC across product lifecycles to include unit, integration, regression, and security (e.g., Security Technical Information Guide (STIG)) testing to ensure the delivery of quality, DOD-compliant products.

C.5.3.7.4.3 GOVERNMENT QUALITY ASSURANCE (QA)

The Government will evaluate the contractor's performance for compliance with the requirements set forth in this TO. The COR, TPOC, and the contractor's representative(s) will meet periodically to review performance and inspect work. These meetings may take place at the place of performance or at an alternate location as determined by the Government. This requirement is not in lieu of the FAR Inspection and Acceptance clause, but in addition to those terms.

C.5.3.8 SUBTASK 8 – CONFIGURATION MANAGEMENT (CM)

C.5.3.8.1 As part of a software assurance process, the contractor shall develop a Configuration Management Plan (CMP) (see Section F, Deliverable #32) and establish and maintain a strict change control process. The change control process shall include Applications, Database, and Updates.

C.5.3.8.2 The contractor shall sustain configuration control and configuration documentation, as well as report configuration status, in accordance with Capability Maturity Model Integration (CMMI) for Development, SEI, August 2006; American National Standards Institute (ANSI)/EIA Standard 649 (National Consensus Standard for Configuration Management); Military Handbook (MIL-HDBK)-61A, Configuration Management Guidance (latest version);

and Assistant Secretary of the Army for Acquisition Logistics & Technology (ASA ALT) Configuration Management Policy, dated 17 November 2011 or current version.

C.5.3.8.3 The contractor shall support CM of requirements such as software and engineering change proposals (ECPs) in response to security vulnerabilities, directed architecture changes, policy/regulatory changes, legislative changes, interface changes, Business Process Improvements (BPIs), environmental changes.

C.5.3.8.4 The contractor shall manage strict version control on all software source code and related artifacts either acquired or developed per the Government-accepted CMP.

C.5.3.8.5 The contractor shall maintain the baselines and documentation for all system releases.

C.5.3.8.6 The contractor shall monitor and report the installation status of each new release.

C.5.3.8.7 The contractor shall utilize a CM tool that is interoperable with Serena Dimensions version 2009R2.

C.5.3.8.8 The contractor shall apply CM through the entire lifecycle of all technology to include:

a. Preparation of CM documentation for enterprise and project artifacts.
b. Participation in CM planning.
c. Oversight and participation in library setup and control for all developmental components and products; participation in the identification and marking of baseline product components.
d. Working with division, project, and Government QA management to identify and resolve quality issues.
e. Participation in process improvement initiatives.
f. Supporting technical configuration control boards.
g. Developing, documenting, and executing CM policies, processes, and standard operating procedures.
h. Document Management - The contractor shall ensure proper control and coordination of all documents generated to fulfill the requirements of this TO such that all data deliverables are on time and fulfill routine requests for published documents (see Section F:
    1. Configuration
    2. Settings Document (see Section F, deliverable #23)
    3. System Documentation (see Section F, deliverable #24)
    4. Application Release/Service Pack Technical Information Packages (TIP) (see Section F, deliverable #25)
    5. Release Plans (see Section F, deliverable #26)
    6. System User Documentation (see Section F, deliverable #27)
    7. System User Documentation – Software User Manual (SUM) and ReadMe (see Section F, deliverable #28)
    8. System User Documentation – Database Software Installation Instructions (see Section F, deliverable #29)

9. System User Documentation – Web Application Server Installation and Administration Guide (WASIAG) (see Section F, deliverable #30)
10. System User Documentation – Database Server Installation Guide (Deliverable #31)

C.5.3.9 SUBTASK 9 – PRODUCT TESTING

C.5.3.9.1 Product testing shall support innovative holistic (entire architecture) solutions within a rapid development and synergistic deployment approach of quality software and hardware. Product testing requires frequent engagement with the end-use community and designated representative testers. Development/testing shall include use of automated regression test techniques as part of a continuous software integration process. The contractor shall ensure all products are thoroughly tested, to include stress and boundary testing, prior to delivery to the Government (see Section F, Deliverable #33). Throughout the software development process, the contractor shall identify and correct product test issues.

C.5.3.9.2 TESTING

C.5.3.9.2.1 The contractor shall conduct appropriate tests consistent with the developmental methodology (e.g., unit, functional, system, interoperability, regression, security, and performance) of software throughout the development lifecycle using industry best practices of continuous integration methods and automated regression test utilities. Test materials (scripts, configurations, utilities, tools, plans, and results) shall be maintained under configuration control.

C.5.3.9.2.2 The contractor shall develop and deliver test procedures, test data, materials, results, and artifacts (see Section F, Deliverable #34) in a format that allows the Government to reproduce the test within their own test environment. The Government will provide only one instance of test data and this test data will be provided during transition-in (see Task 1). The contractor shall maintain and update this one provided instance of the test data for future use; the Government will not provide any other instances of test data.

C.5.3.9.2.3 The contractor shall conduct tests related to non-functional requirements (e.g., load, performance, and installation testing).

C.5.3.9.2.4 The contractor shall correct software defects throughout the software development process identified through testing (including unit, system, functional, security, performance, and load testing) procedures.

C.5.3.9.2.5 The contractor shall include the RCAS TPOC as part of the iteration tests/demonstrations as required.

C.5.3.9.2.6 The contractor shall document systems and application performance and load data as part of testing process (see Section F, Deliverable #35). This data shall be made available upon Government request.

C.5.3.9.2.7 Test scripts, utilities, execution, and results shall be historically maintained under configuration control for comparison and analysis and delivered to the Government upon

request.

C.5.3.10 SUBTASK 10 – GOVERNMENT SECURE TEST ENVIRONMENT (STE)

C.5.3.10.1 Upon delivery of source codes, build materials and related artifacts by the contractor to the STE, source code evaluation and scanning, installation instructions, and testing (functional, security, load, performance, etc.) will be conducted within the STE, which will be hosted by the contractor within the Contractor Environment (Task 5, C5.5). The STE will leverage an existing test environment that is utilized by the contractor in support of the standard release delivery lifecycle. The contractor shall be available to address any issues encountered during installation of test media, test execution, or resolve any problems with the applications as requested.

C.5.3.10.2 The contractor shall provide media (see Section F, Deliverable #36) for all source code, installation kits, software, documentation (including those related to architecture, test design and test results, and installation procedures) and build procedures/scripts in a secure manner at the end of each update or as requested by the Government.

C.5.3.10.3 The contractor shall document in the SDP third-party products used to develop, operate, and construct the software applications.

C.5.3.11 SUBTASK 11 – SOFTWARE DEPLOYMENT MANAGEMENT

C.5.3.11.1 The contractor shall assist the Government in developing a software deployment roadmap that encompasses the individual detailed project plans.

C.5.3.11.2 The software detailed project plans shall include the following content:

a. Software Version Description Document that includes the content of each updated and any known limitations.
b. Unique identifiers for each update.
c. Installation instructions and update media.

C.5.3.11.3 The contractor shall assist the Government in developing an integrated software deployment management solution that ensures simplicity in update installation and system use and reduces the implementation burden on units in the field.

C.5.3.11.4 The contractor shall assist the Government in identifying and implementing a System Lifecycle methodology that provides identification, development, design, testing, training, and implementation of all established requirements.

C.5.3.11.5 The contractor shall ensure their software deployment management practices and processes are complementary to Government practices and processes.

C.5.3.12 SUBTASK 12 – INFORMATION ASSURANCE (IA)

C.5.3.12.1 IA SECURITY ENGINEERING

C.5.3.12.1.1 The contractor shall provide security engineering support in accordance with all DOD and agency-specific security initiatives.

C.5.3.12.1.2 The contractor shall be responsible for identifying and recommending IA security requirements during the entire lifecycle for all systems under this TO.

C.5.3.12.1.3 The contractor shall evaluate and provide innovative recommendations for implementation of IA practices and tools to ensure the latest security practices are being employed (in accordance with (IAW) extant Army standards).

C.5.3.12.1.4 The contractor shall monitor, and evaluate IA-related list services such as Information Assurance Support Environment (IASE) and Army Computer Emergency Response Team (ACERT) portal to ensure the most current information is being utilized to maintain a secure baseline.

C.5.3.12.1.5 The contractor shall accommodate changing information security requirements and emerging technologies by proposing, updating, and revising existing architecture designs to incorporate and address evolving requirements.

C.5.3.12.1.6 The contractor shall provide and maintain a configuration settings document (see Section F, Deliverable #37) that describes how each IA finding is resolved or mitigated.

C.5.3.12.1.7 The contractor shall acquire COTS and GOTS components for security functions (excluding cryptographic modules) in accordance with policies and guidance contained in the DOD IT Standards and Profile Registry (DISR), https://disronline.csd.disa.mil/ (requires Common Access Card (CAC) for access).

C.5.3.12.1.8 The contractor shall conduct scans and vulnerability assessments and implement fixes for all vulnerabilities identified. The contractor shall deliver vulnerability assessment documented analysis reports at least quarterly or upon the release of updated or new Security Technical Implementation Guide (STIG) and Security Readiness Reviews (SRRs) applicability.

C.5.3.12.1.9 The contractor shall support the implementation of all CAC and Public Key Infrastructure (PKI) initiatives.

C.5.3.12.1.10 The contractor shall specifically address IA considerations with every system change recommendation.

C.5.3.12.2 SECURITY MANAGEMENT

C.5.3.12.2.1 The contractor shall establish a security program in accordance with Army regulation (AR) 25-2 (http://www.apd.army.mil/pdffiles/r25_2.pdf), DODD 8500.1 (http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf), DODI 8500.2 (http://www.cac.mil/docs/DoDD-8500.2.pdf). The contractor shall also ensure that security is integrated and enforced in all phases of the software development process.

C.5.3.12.2.2 The contractor shall support Army Certification and Accreditation (C&A) activities that include DIACAP or Defense Information Assurance Risk Management Framework (DIARMF) activities.

C.5.3.12.2.3 The contractor shall maintain a Continuity of Operations Plan (COOP) (see Section F, Deliverable #39) for the development environment and the production and the technical infrastructure of RCAS USARC activities at Fort Bragg and any other CONUS location designated.

C.5.3.12.2.4 The contractor shall ensure that the USARC RCAS operational environment located at Fort Bragg, NC maintains a high state of IA compliance by monitoring and applying all applicable Defense Information Systems Agency STIGs and security-related patches approved for implementation within Government-established suspense dates.

C.5.3.12.2.5 The contractor shall conduct annual audits in accordance with DOD 8500.2 and AR 25-2 for RCAS IA controls that will audit at least 33% of all applicable controls at the USARC site. The contractor shall provide an annual review report of the audit. The contractor shall ensure that at the end of a three year period, 100% of all IA controls are evaluated.

C.5.3.12.2.6 The contractor shall maintain adherence to all applicable DOD and Army policies, regulations, and guidelines relating to IA.

C.5.3.12.3 IA SECURITY RISK REMEDIATION AND MITIGATION

C.5.3.12.3.1 The contractor shall develop an IA strategy (see Section F, Deliverable #40) that describes concisely how a program's IA features comply with applicable Federal, DOD, and the National Guard standards, regulations, and requirements. The IA strategy shall briefly describe the system, the program's risk assessment in the face of cyber and physical threats, the acquisition strategy, and the certification and accreditation approach. The Government anticipates that the IA strategy should evolve as a program matures.

C.5.3.12.3.2 The contractor shall provide input to the Government in support of required Plans of Action and Milestone (POA&M) submissions, identifying risks in support of the Government's remediation and mitigation plan of action throughout the POA&M process.

C.5.3.12.3.3 The contractor shall perform audits of production assets to maintain and ensure compliance. The contractor shall provide guidance and recommendations on implementation of new or updated STIGs and SRRs.

C.5.3.12.3.4 The contractor shall comply with all applicable Information Assurance Vulnerability Management (IAVM) policies and tools prescribed by DOD and Army policy.

C.5.3.12.3.5 The contractor shall assist the Government in submitting and correcting the Certificate of Noteworthiness (CoN) (AR 25-1) application (see Section F, Deliverable #41) required by Netwotk Command (NETCOM) for the applications, systems, networks, and/or information systems. The contractor shall follow CoN instructions put forth by NETCOM for this requirement.

C.5.3.12.3.6 The contractor shall perform automated scans and manual checks as applicable on the USARC RCAS servers.

C.5.3.13 SUBTASK 13 – REQUIREMENTS MANAGEMENT

C.5.3.13.1 The contractor shall provide requirements management support including documenting, sequencing, and traceability of functional requirements (see Section F, Deliverable #42).

C.5.3.13.2 The contractor shall deliver and maintain a requirements management process acceptable to the Government to manage and account for changes in the systems requirements.

C.5.3.13.3 The contractor shall update documentation such as Context Diagrams, Use Case Models, and associated design documentation for new requirements and iterations of an application system. The contractor shall assess and document the impact of new functional requirements on the existing design baseline. The contractor shall ensure that any changes to the application design are in conformance with the Human Factors Engineering of Computer Workstations ANSI/HFS 100-2007 (http://www.hfes.org/Publications/ProductDetail.aspx?ProductID=69).

C.5.3.13.4 The contractor shall complete Engineering Change Proposal (ECP) analyses in accordance with the methodologies and timelines contained within the SDP. The Government expects these analyses to be timely and thorough and have no impact on other software-related activities.

C.5.3.14 SUBTASK 14 – ASSET MANAGEMENT

C.5.3.14.1 The contractor shall utilize processes and methodologies to safeguard and maintain full visibility and accountability of all Government equipment and tools, deployed hardware, software, IT assets, and COTS software license and warranty management information placed under the contractor's control.

C.5.3.14.2 The contractor shall store, track the shipment and receipt of, and dispose of Government property in accordance with FAR Part 45 (Government Property).

C.5.3.14.3 The contractor shall assist the Government with obtaining National Stock Numbers (NSNs) for equipment and properly transfer accountability of the equipment (https://acc.dau.ml/CommunityBrowser.aspx).

C.5.3.14.4 The contractor shall utilize the standard Army Asset Management System, Property Book Unit Supply – Enhanced (PBUS-E). Individuals assigned the task of entering data into PBUS-E shall access military networks and therefore require elevated privileges.

C.5.3.14.5 The contractor shall perform inter and intra-site equipment relocations.

C.5.3.14.6 The contractor shall deliver a yearly inventory of all GFE in the control of the contractor (see Section F, Deliverable #43).

C.5.3.15 SUBTASK 15 – ENTERPRISE TRAINING AND DOCUMENTATION

C.5.3.15.1 The contractor shall deliver enterprise training to include sustainment of current and new training initiatives (see Section F, Deliverables #44, 45, 46, and 47). The contractor shall maintain all applicable documentation, including delivery methods, user documentation, and current training materials.

C.5.3.15.2 The contractor shall develop and maintain to current, new equipment training (NET) materials and other associated instructional support materials (see Section F, Deliverable #48) leveraging Distance Learning (DL) methodologies to include Distributed Learning (dL) courseware.

C.5.3.15.3 The contractor shall develop, sustain, and update the PD's library of DL products (see Section F, Deliverable #49) provided as GFI to ensure all RCAS training is applicable to the current production environment.

C.5.3.15.4 The Contractor shall ensure quality production of Interactive Multimedia Instruction (IMI), in accordance with U.S. Army Training and Doctrine Command (TRADOC) Regulation 350-70-2 (http://www.tradoc.army.mil/tpubs/index.htm), for the specified PD RCAS courses and corresponding tasks.

C.5.3.15.5 The contractor shall develop and maintain DL courseware IAW TRADOC IMI standards (see Section F, Deliverable #50) that is doctrinally correct and uses performance-based learning techniques with appropriate levels of interactivity and practical exercises to inform attendees. The courseware will be hosted on the Army Learning Management System (ALMS) and the National Guards' Guard University (GuardU).

C.5.3.15.6 The contractor shall coordinate testing of the final courseware modules – to include Sharable Content Object Reference Model (SCORM) conformance, ALMS and GuardU

playability, and Blackboard playability–with responsible government organizations, in coordination with the FEDSIM COR and TPOC.

C.5.3.15.7 The contractor shall deliver and maintain user access to appropriate training equipment, materials, and documentation in a cost-effective manner that provides for rapid availability within ten days of acceptance by the Government of all software releases.

C.5.4 TASK 4 – RCAS SUPPORT (FFP)

The contractor shall perform systems engineer (SE) functions (see Section F, Deliverables #51 and 52) to include field support, Enterprise Service Desk, system and data-based administration and Tier 2 Voice over Internet Protocol (VoIP) Help Desk Support at USARC, training server management, USARC COOP support, special project support, and trainers. All personnel assigned to these tasks require access to military networks and elevated privileges. As a result, all personnel assigned to these tasks must meet the requirements in C.5.3.12.2, Security Management. Specific tasks and responsibilities are described below.

C.5.4.1 SUBTASK 1 – ENTERPRISE SERVICE DESK

C.5.4.1.1 The contractor shall provide a tiered (not including Tier 1) Enterprise Service Desk that shall include telephonic and on-site (as required) / live system engineering support. This support responds to end-user requests and shall be integrated with the existing ARNG Remedy Action Request system (ARS) (currently version 7.1 and Information Technology Service Management (ITSM) version 5.6), USAR CA Unicenter (currently version R12.5), and Tier 1 service desk operations and processes. The contractor shall identify customer problems and implement repeatable, best-practice solutions across the enterprise.

C.5.4.1.2 The contractor shall monitor the problem resolution process from initial contact to post-resolution end-user feedback. The contractor shall provide *live* coverage from 0700 to1700 Eastern Time (ET), excluding weekends and federal holidays. The contractor shall be responsible for providing support for the following functions:

- RCAS-developed GOTS
- RCAS Web
- Database
- Supporting COTS (e.g., Server 2008, IIS, Oracle, VM)
- External Interface
- Sustaining Engineer Request
- Media Request
- Other support functions specifically in-scope of this TO

C.5.4.1.3 The contractor shall perform root cause analysis for Tier 2 and Tier 3 trouble tickets as necessary. The contractor shall create and maintain updated on-line information about known root causes and their symptoms (see Section F, Deliverables #53 and 54).

C.5.4.2 SUBTASK 2 – FIELD SUPPORT

C.5.4.2.1 The contractor shall provide subject matter expertise to address technical issues that cannot be resolved at lower tiers of the Enterprise Service Desk. This support shall include remote and on-site system engineering support for RCAS applications, fielded COTS, and hardware issues. The Government anticipates significant CONUS travel associated with this sub-task (see Section J, Attachment X, Field Support Travel History).

The contractor shall:

a. Evaluate software application issues on site and in the field.
b. Conduct analyses on technical issues and provide engineering support for architecture issues as they pertain to the development of software applications and hardware implementations.
c. Effectively communicate issues and resolutions to all levels of the organization.
d. Interact with internal and external customers.
e. Provide technical support and advice to ensure program/project objectives are met.
f. Produce innovative solutions for a variety of complex problems.
g. Assist in formulating requirements; advise on alternatives and on the implications of a newly revised system.
h. Identify omissions and errors in requirements and recommends optimum approaches.
i. Provide technical assistance to the sustaining engineers (SE) staff.

C.5.4.2.2 The contractor shall provide support to the Government's strategic communications by providing technical information and demonstrations regarding application initiatives and technical updates as needed. The contractor shall also provide input for inclusion to the PD RCAS newsletter and support customer conferences and workshops as required.

C.5.4.3 SUBTASK 3 – USARC OPERATIONS

The contractor shall provide server and database support to the RCAS enclave. The Contractor shall adhere to the DA Pamphlet 25-1-1, Service Level Agreement (SLA) between the USARC G6 and PD RCAS for hosting RCAS production and training environments on the USARC Unified Computing System. Contractor support shall be provided from 0700 to1700 ET, excluding weekends and federal holidays.

C.5.4.3.1 The contractor shall provide system administrations capabilities for operations and maintenance of the RCAS production servers, staging servers, COOP servers, and training servers located at Fort Bragg, NC. This support includes configuring all new implementations and developing processes and procedures for ongoing management of the RCAS server environment and related components to achieve consistent and reliable performance of the various RCAS applications. This support shall ensure the availability and reliability of the RCAS suite of applications and, where applicable, coordinate with the database administrator (DBA) to ensure the integrity of the RCAS databases.

The Contractor shall:

a. Install applications and configure the operating system within the UCS environment.
b. Ensure all servers are IAVA and STIG compliant. Install/update all O/S patches as required.
c. Perform security checklists on operating systems and system backups for each server.
d. Perform daily server operations and maintenance.
    1. Perform server troubleshooting.
    2. Monitor system logs, security logs, and application logs.
    3. Perform detailed monitoring and tuning.
    4. Provide file transfer, archiving, data backup and restoration.
e. Provide server and application operation and maintenance support for functional staff specific applications.
f. Perform daily training server operations: maintain and administer student accounts,
g. Develop processes and procedures.
h. Keep servers up to date with the most current fielded application baseline.

C.5.4.3.2 The contractor shall provide database administration including the design, implementation, maintenance, and repair of the USARC environment. This includes the development and design of database strategies, monitoring and improving database performance and capacity, and planning for future expansion requirements. DBA support shall also involve planning, coordinating, and implementing security measures to safeguard the database.

The contractor shall:

a. Install and upgrade the Oracle server and application tools.
b. Allocate system storage and planning for future storage requirements for the database system.
c. Create primary database storage structures (table spaces) (see Section F, Deliverable #55) after application developers have designed an application.
d. Create primary objects (tables, views, indexes) (see Section F, Deliverable #56) once application developers have designed an application.
e. Modify the database structure, as necessary, from information given by application developers.
f. Enroll users and maintain system security.
g. Ensure compliance with Oracle license agreement.
h. Control and monitor user access to the database.
i. Monitor and optimize the performance of the database.
j. Plan for backup and recovery of database information.
k. Backup and restore the database.
l. Coordinate with Oracle Corporation for technical support.

C.5.4.3.3 (Optional) The contractor shall provide Tier 2 Help Desk support for the USAR ITII&R VoIP. The USAR voice services solution toolset currently consist of Cisco Unified Communications Manager (CUCM) and Cisco Communications Manager Express (CME), version 8.x.

At the start of the task order, PD RCAS anticipates a total of 84 sites (79 CME and 5 CUCM) with approximately 7740 users (4740 CME and 3000 CUCM) will require support.

The contractor shall support trouble tickets escalated by the USARC G2/G6 Tier 1 support provider Verizon Business Technical Assistance Center (VB TAC) (see Section F, Deliverable #54). Contractor support shall be on-site and shall be live coverage from 0700 to1700 ET, Monday through Friday. Weekend support for drills may be required if USARC is concerned about a high risk of service interruption.

The contractor shall:
a. Make moves, adds, and changes to router and voice mail configurations.
b. Troubleshoot and maintain IP Telephony/Unity.
c. Troubleshoot Layer 2 telephony transports (ISDN PRI, TI, DS-3, etc.).
d. Provide CUCM 8.x support.
e. Provide analog configurations and troubleshooting support.

The contractor shall develop a CUCM and CME user's manual and training material for distribution and use by USAR G6 support staff and site facility management (see Section F, Deliverable #57).

C.5.4.4 SUBTASK 4 – USARC COOP SUPPORT

The contractor shall deliver subject matter expertise to support the Fort Bragg site in the event that COOP is implemented and services are moved to the backup location. Contractor support shall involve assisting in the performance of the responsibilities of the Fort Bragg site personnel to include System Administrator (SA)/DBA responsibilities. The contractor shall ensure that COOP servers are maintained at the proper RCAS update level and that all IA controls are in place. The contractor shall ensure specific duties/responsibilities and alternate work locations are outlined in the USARC SOP, MOA and RCAS COOP documentation.

The contractor shall:
a. Evaluate software application issues on site and in the field.
b. Conduct analyses on technical issues and provide engineering support for architecture issues as they pertain to the development of software applications and hardware implementations.
c. Apply all applicable software patches/upgrades in accordance with IA process.
d. Coordinate and install RCAS releases in coordination with Fort Bragg outage schedules.
e. Troubleshoot end-user issues/trouble tickets as applicable.
f. Effectively communicate issues and resolutions to all levels of the organization.
g. Interact with internal and external customers.
h. Ensure that all applicable IEs are updated to point to servers in event COOP is activated.
i. Participate in COOP-related training and exercises.
j. Produce innovative solutions for a variety of complex problems.
k. Assist in formulating requirements; advise on alternatives and on the implications of a newly revised system.

l. Identify omissions and errors in requirements and recommends best practices.
m. Plan work schedules and perform customer support activities involving software design, developments, testing, and program management.

C.5.4.5 SUBTASK 5 – TRAINING SERVER ENCLAVE

The contractor shall deliver subject matter expertise for the operational support and maintenance of the RCAS Training Servers to include system security, systems monitoring, troubleshooting, repair, performance evaluation, applying RCAS updates and patches, and creating student accounts for soldiers attending RCAS functional training. The training environment located at Fort Bragg consists of Level 1 and Level 2 web and database servers that support all RCAS training for the Guard and Reserve.

The contractor shall:
a. Perform backups
b. Test backups
c. Perform service availability monitoring
d. Perform event log monitoring
e. Perform drive space monitoring
f. Perform log file maintenance
g. Perform patch level monitoring and management
h. Develop and maintain documentation
i. Manage IA and Security

C.5.4.6 SUBTASK 6 – SPECIAL PROJECT SUPPORT

The contractor shall deliver subject matter expertise to support special projects as required. Historically, support has been in relation to technical initiatives as identified by the RCAS program. The contractor shall provide technical and functional support in relation to the fielding of new COTS and hardware to the field. Historically, responsibilities associated with this sub-task have included documentation review/redlines, troubleshooting software/hardware issues while onsite, training end-users on use of new software/hardware, installing new hardware, and migration of servers across domains. Historically, special projects have been in support of the Active Component, Guard, and Reserve.

The contractor shall:
a. Evaluate software application issues on site and in the field.
b. Conduct analyses on technical issues and provide engineering support for architecture issues as they pertain to the development of software applications and hardware implementations.
c. Travel as required to customer sites to install new software/hardware.
d. Provide training to end-users on use of new software/hardware.
e. Effectively communicate issues and resolutions to all levels of the organization.
f. Interact with internal and external customers.
g. Monitor activities and schedules.

h. Produce innovative solutions for a variety of complex problems.
i. Assist in formulating requirements; advise on alternatives and on the implications of a newly revised system.
j. Identify omissions and errors in requirements and recommends optimum approaches.
k. Assist in the development and testing of systems design for approved technical initiative projects.
l. Plan work schedules and perform customer support activities involving software design, developments, testing, and program management.
m. Review documentation and provide documentation of errors/anomalies (redlines as applicable).

C.5.4.7 SUBTASK 7 – CONDUCT TRAINING

The contractor shall provide a high-quality, reliable approach to end user training. The contractor shall conduct classes IAW all applicable TRADOC standards. The contractor shall conduct classes on all RCAS applications at a variety of sites to include the Professional Education Center (PEC), Little Rock, AR, the Army Reserve Readiness Training Center (ARRTC), Fort Knox, KY, and other sites for units within the Reserve Component (RC). The classes depicted in the chart below shall be offered on a yearly basis.

Trips	Classes (Can run concurrently)	Locations (Government Provided)	Curriculum
2	2-4	PEC	All RCAS application
2	2-4	ARRTC	All RCAS application
2	4	West Coast	All RCAS application
2	4	East Coast	All RCAS application

Note: Currently, class size averages 12-20 students per class.

C.5.5 TASK 5 – CONTRACTOR ENVIRONMENT (FFP)

C.5.5.1 SUBTASK 1 – ESTABLISH DEVELOPMENT AND INTEGRATION ENVIRONMENT

C.5.5.1.1 The contractor shall provide a development and integration environment. The contractor shall submit a detailed plan (see Section F, Deliverable #58) and associated costs for establishing an isolated software development and test environment that includes, but is not limited to, hardware, software, automated tools, licenses, maintenance, and life cycle

management. Current hardware performance and storage characteristics of the development and test environment are identified in Section J, Attachment Y.

C.5.5.1.2 The software development and integration environment shall be logically isolated from other networks, to include corporate enterprise and other unclassified networks. Software deliveries shall consist not only of the software update and associated installation materials, but also all related source and installation build instructions and utilities sufficient to reconstruct the installation media, test installation, and perform testing.

C.5.5.1.2.1 All development shall be performed at the contractor's isolated development environment. The contractor's development environment shall conform to the following guidelines:

a. The development environment shall be logically isolated from other networks, to include corporate enterprise and other unclassified networks.
b. Security Program guidelines for the environment shall be prepared and delivered to the Government for review and approval before developing any software.
c. The Security Program implemented shall use the security controls described in National Institute of Standards and Technology (NIST) Special Publication 800-53 (dated August 2009, or latest revision), *Recommended Security Controls for Federal Information Systems and Organizations as a guide*.
d. The development environment shall be isolated and protected via Government approved firewall technology from the contractor's corporate (and other) network, and when accessed remotely, meet the Army standards for remote access.
e. The secure IDE referenced in section C.5.3.4.1 that includes a real-time, collaborative environment that enables access to the contractor's (or an associated sub-contractor's) software development environment shall meet the Army Password Standards, version 2.5, dated 1 May 2008.

C.5.5.1.3 FIREWALL PROTECTION

The contractor shall ensure the development environment is isolated and protected via Government-approved firewall technology from the contractor's corporate (and other) networks and, if accessed remotely, using an encrypted Virtual Private Network (VPN) from Government compliant dedicated workstations.

C.5.5.1.4 ACCESS TO LOGS

Firewall access logs are required to permit the Government to monitor and analyze cyber threats and risks, especially in the advent of a cyber event. The contractor shall provide authorized Government stakeholders on-demand access to firewall access logs.

C.5.5.1.5 SELF-CONTAINED

The contractor shall ensure the environment contains all developmental products and services necessary to conduct development activities within the isolated environment, including source code library management, program management, team collaboration, testing, and development tools and applications; no publication of RCAS intellectual property shall be exposed beyond the isolated network, other than those networks directed by the PD RCAS. Configuration management and monitoring/auditing controls and procedures shall be instituted to ensure that RCAS intellectual property is not exposed beyond the isolated network. The Contractor shall maintain virtual images of current and future software baselines within its development environment.

C.5.5.2 SUBTASK 2 – OFFICE AUTOMATION

The contractor's office automation software must be compatible with the current version of the Army Gold Master suite of software.

C.5.5.3 SUBTASK 3 –ASSET MANAGEMENT

The contractor shall have the capability of receiving, staging, configuring, storing, and shipping equipment to primarily support MILCON and DLP operations. Volume is directly impacted by operational tempo, what is being fielded, and available funding. The preponderance of the RCAS-core fielded equipment is direct shipped from the vendor to unit/customer locations.

The contractor shall comply with all local, state, and Federal codes, regulations, and laws concerning workplace safety and well-being of warehouse personnel. Refer to www.osha.gov for additional information and regulatory guidance.

The contractor shall store, track the shipment and receipt of, and dispose of Government property in accordance with FAR Part 45 (Government Property).

The contractor shall utilize the standard Army Asset Management System, Property Book Unit Supply – Enhanced (PBUS-E). Individuals assigned the task of entering data into PBUS-E shall access military networks and therefore require elevated privileges.

C.5.6 TASK 6 – HARDWARE AND SOFTWARE PRODUCTS (FFP)

The contractor, in coordination with, and with approval from, the FEDSIM COR and TPOC, shall procure hardware and software products to support elements of the ARNG and USAR in the field.

Procurement shall incorporate methods for economically delivering COTS products to the Government. The contractor shall provide for economies of scale and ensure chosen technologies and products perform to the current and anticipated technological environments.

The contractor shall provide the Government with purchase requests (see Section F, Deliverable #59) for all required procurement actions. These requests must include the total cost of the procurement action to include, but not be limited to, the direct unit cost and extended cost for each material item, as well as any indirect costs, including profit, but primarily labor associated with such activities as market research, pricing analysis, contracting, shipping and handling, and asset management associated with this purchase.

C.5.6.1 SUBTASK 1 – PURCHASING

All purchases shall be consistent with DOD and Army Acquisition Policies (e.g., the use of the Army Computer Hardware Enterprise and Software Solutions (CHESS) contract vehicles as the primary source for purchases).

C.5.6.2 SUBTASK 2 – PRODUCT ASSEMBLY AND SHIPMENT

The preponderance of procurement actions will involve direct shipping from the vendor/original equipment manufacturer (OEM) to the specific ARNG or UASR destination. However, consistent with the consent to purchase guidelines (see Section H.24), the Contractor may be required to pre-assemble/assemble, integrate, prepare for shipment, and ship product components to designated locations.

C.5.6.3 SUBTASK 3 – PRODUCT INSTALLATION

The contractor shall provide processes and methodologies necessary to systematically deliver, install and account for equipment to fully equip or retrofit sites designated by the Government. Installation may involve fabrication of mounts, brackets, and installation kits. The contractor shall provide recommendations to the Facilities Maintenance Officer (FMO) regarding electrical power, space, and lighting requirements, as well as other architectural, logistical, and facility planning considerations. The contractor shall provide information technology (IT) support to operational sites (such as incident command centers) for items (e.g., monitors, data lines, and video teleconferencing (VTC) capability). The contractor shall coordinate the installation of equipment and all other contractor services, to include site surveys, necessary to complete the installation for each of the designated sites.

C.5.7 TASK 7 – IT INFRASTRUCTURE INTEGRATION AND REFRESH (ITII&R)

C.5.7.1 SUBTASK 1 – PLANNING AND DESIGN (P&D) (CPAF)

The appropriate military organization (e.g., USARC G2/G6) is responsible for providing the necessary GFI in order to design and subsequently install an IT solution at identified locations. The requirements provided by the GFI will allow the contractor to classify the IT project size (i.e., small, medium, or large). A small project is defined to be a site where the IT implementation funding estimate specified in the GFI is no more than $150,000. A medium project is a site where the IT implementation funding estimate specified in the GFI is between

$150,000 and $250,000. A large project is a site where the IT implementation funding estimate specified in the GFI is greater than $250,000. The contractor should anticipate an average of 30 projects per annum.

Upon contractor arrival at the installation site, the PBO (or Government designee per the DA For 1687) and contractor representative will perform a joint inventory of the equipment and sign the DD Form 250 (see Section F, Deliverable #61) and if necessary, the DD 1149.

C.5.7.1.1 The IT funding estimate is based on factors such as unit/soldier counts and IT service ports. The contractor shall provide cost estimates including labor, travel, and Lists of Materials (LOM) to support each site's data and voice requirements along with its associated network connectivity diagram.

C.5.7.1.2 The contractor shall staff this effort to allow multiple site designs to be developed simultaneously in accordance with the list of sites provided by the Government. The Planning and Design (P&D) subtask is limited to the engineering design that includes a site-specific cost estimate for each site. Implementation of the data and voice solution for each site that will be implemented under this estimate will be performed as separate tasks proposed at a later date. Examples of the design and LOM for each sized effort are located in Section J, Attachment AO.

The following is a list of minimum tasks the contractor shall perform in order to produce an IT network design:

a. Assist the Government in gathering and posting site-specific GFI data.
b. Review and analyze supporting documents posted on websites.
c. Work to complete the design based upon assumptions and historical data in lieu of any missing GFI data.
d. Accomplish site-specific equipment sizing using the GFI for the data network and, if required, voice network.
e. Develop site-specific equipment LOMs (see Section F, Deliverable #60) to field the local area data network and, if required, voice network to implement the engineering design requirements.
f. Develop site-specific labor cost estimates to configure, test, ship, and install the hardware to implement the engineering design requirements.
g. Populate the Site Cost Estimate Worksheet and finalize all summary cost data.
h. Document the LOM within the Site Cost Estimate Worksheet and include network connectivity diagrams upon completion of each site's initial engineering design review process.

C.5.7.2 SUBTASK 2 – NETWORK INSTALLATION (FFP)

The contractor shall purchase the necessary equipment and tools, configure/test the equipment, ship the equipment to the project location, and conduct the network installation previously designed under Task 7, Subtask 1 of this order. All personnel assigned to this task require access to military networks and elevated privileges.

C.5.7.2.1 The contractor shall ship equipment/tools to a specific site Property Book Officer (PBO) as identified on the Department of the Army (DA) Form 1687. The site PBO will be identified prior to any shipment of equipment. The PBO will safeguard the equipment/tools at the site until the contractor's Installation Team arrives. Upon contractor arrival at the installation site, the PBO (or Government designee per the DA Form 1687) and contractor representative will perform a joint inventory of the equipment and sign the DD Form 250 (see Section F, Deliverable #61).

C.5.7.2.2 The Contractor shall be responsible for the on-site IT network installation and conduct the necessary testing to confirm operability; operability will be confirmed by an assigned (local) Government technical representative.

C.5.7.2.3 The Contractor shall complete the following checklists (after installation is complete and ready for site network turnover):

a. Walk-Through Checklist (Section F, Deliverable #63)
b. Post-Installation Checklist (Section F, Deliverable #64)
c. Customer Satisfaction Questionnaire (Section F, Deliverable #62)
d. Test Procedure Checklist (Section F, Deliverable #65)
e. The contractor's delivery of "As Built Network Drawings" to Government Configuration Management (CM) (Section F, Deliverable #66)

C.5.7.2.4 The contractor shall conduct weekly meetings with the RCAS PD in order to communicate project status and identify issues.

C.5.7.2.5 The contractor shall prepare and submit Site Status reports (Section J, Attachment AM) (see Section F, Deliverable #67).

C.5.7.2.6 The contractor shall attend regularly scheduled project coordination and status meetings in person with the staff of the military organization (e.g., USARC G2/G6 and the Assistant Chief of Staff for Installation Management (ACSIM) organizations). These meetings are currently scheduled quarterly. The contractor shall prepare and deliver meeting minutes (see Section F, Deliverable #68) to record the results of these meetings.

C.5.7.2.7 The contractor shall attend quarterly Engineering Program Reviews (EPR) conferences. These conferences are currently sponsored by the U.S. Army Corps of Engineers, but may include other organizations in the future. The status of all aspects of a site's construction is reviewed to include IT implementation activities applicable to this TO. The quarterly project coordination and status meeting is frequently held during the EPR since representatives from the Government are in attendance.

C.5.8 TASK 8 – DISTRIBUTED LEARNING PROGRAM (DLP) CORE SUSTAINMENT (CPAF)

This task requires daily usage of the ARNG Remedy ARS to open, track, update, and close field support tickets and provide remote VTC and telephonic real-time functional troubleshooting.

C.5.8.1 SUBTASK 1 – HELP DESK

The contractor shall provide Enterprise Service Desk support. The contractor shall integrate its support with existing ARNG service desk operations and processes. The contractor shall identify customer problems and solutions and maintain corrective procedures that are repeatable across the enterprise.

C.5.8.1.1 The contractor shall review, modify, and develop standards and procedures for the problem resolution process (see Section F, Deliverable #69); this includes focusing on customer call reduction and the use of root cause analysis. The contractor shall perform Tier 2 field support for the DLP.

C.5.8.1.2 The contractor shall monitor the problem resolution processes. The contractor shall measure performance and analyze data to isolate and solve computing, security, and networking problems.

C.5.8.1.3 The contractor shall include help-desk root cause analysis and help desk statistics (i.e., trouble tickets opened, in process, and resolved; metrics regarding response time to trouble ticket resolution) in the contractor's monthly status reports (see Section F, Deliverable #54).

C.5.8.2 SUBTASK 2 - SUSTAINING ENGINEERING

The Contractor shall be responsible for providing Sustaining Engineering subject matter expertise support to activities that include leveraging 132.xx network access to perform Tier 3 field support and resolution of escalated DLP operational classroom issues (workstation, audio video and video teleconferencing), identification of product end-of-life and support candidates, evaluation of submitted deviations and waivers. The Contractor shall maintain the Classroom Baseline and Hardware Matrices (see section F, deliverable #70).

C.5.8.2.1 The Contractor shall conduct engineering studies (see section F, deliverable #71) and analysis to support DL classrooms/capabilities, engineering analysis to support IPV6 conversion, analysis of IA and accreditation support activities, and analysis of support for future DLP software images based on AGM updates. The Contractor shall be prepared to support classroom improvements or modernization including the list of deliverables below:

a. Classroom Refresh Plan; see section F, deliverable #72
b. Classroom Installation Fielding Requirements Engineering Document (FRED); see section F, deliverable #73
c. DLP Integration Manual; see section F, deliverable #74
d. DLP Installation Manual; see section F, deliverable #75

The contractor shall sustain functionality of the complete family of in-service hardware and software products, and shall ensure that security and product updates, quality releases, patches, fixes, and service packs are installed in accordance with the manufacturer's recommendations.

C.5.8.3 SUBTASK 3 - EQUIPMENT MAINTENANCE

The contractor shall provide DLP equipment maintenance support to include leveraging 132.xx (GuardNet) network access to perform Tier 4 field support, resolve escalated DLP break-fix tickets for DLP classroom components using a planned resources and spares inventory, to ensure that the failure of critical classroom components (e.g., Crestron AV controller, touch panel, Tandberg CODEC, matrix switcher) does not render the classrooms unusable or unavailable/offline.

C.5.8.3.1 The contractor shall provide support for other activities performed in support of this equipment maintenance to include ensuring repair of failed components, shipping replacement components (i.e., generating DD Form 1149), issuing/monitoring equipment manufacturer Return Material Authorizations (RMAs), procuring spares/maintenance equipment in support of field failures, establishing and tracking of equipment warranties, performing periodic equipment inventories, and providing equipment failure trend monitoring and analysis.

C.5.8.4 SUBTASK 4 – ENTERPRISE SUPPORT

The contractor shall provide support for enterprise activities of quality assurance and metrics, risk management and lessons learned programs/data repositories, programmatic configuration management, programmatic asset management, facilities management, lab management, test and evaluation management, enterprise customer relationship management, liaison activities, and portal management.

The contractor shall store, track the shipment and receipt of, and dispose of Government property in accordance with FAR Part 45 (Government Property).

The contractor shall utilize the standard Army Asset Management System, Property Book Unit Supply – Enhanced (PBUS-E). Individuals assigned the task of entering data into PBUS-E shall access military networks and therefore require elevated privileges.

C.5.8.4.1 The contractor shall ensure COTS software and hardware is fully compatible with DOD's Shareable Content Object Reference Model (SCORM). The systems architecture includes all software, telecommunications, satellite, audio, video, multimedia, networking, server, and desktop hardware.

C.5.9 TASK 9 – IMA CORE SUSTAINMENT (CPAF)

C.5.9.1 SUBTASK 1 – PLANNING AND IMPLEMENTATION OF SOFTWARE

Section C.5.3.1 applies to this subtask.

C.5.9.2 SUBTASK 2 – ESTABLISH DEVELOPMENT ENVIRONMENT

Section C.5.5 applies to this subtask.

C.5.9.3 SUBTASK 3 – SUSTAINMENT SUPPORT

C.5.9.3.1 The contractor shall gain an in-depth understanding of the overall system architecture, data flow, and system design and functionality requirements to include system of system interfaces. The contractor shall sustain system baselines and provide system engineering and maintenance in support of the ARNG enterprise applications. The contractor shall make sure all baseline changes are accurately captured and reported to the system of record. Examples of baseline changes include work products involving hardware, software, database, information exchange, security, and documentation. The contractor shall sustain functionality of the complete family of hardware and software products, ensuring timely security and product updates and quality releases are managed efficiently and effectively.

C.5.9.3.2 The contractor shall provide an interactive, user-driven development methodology characterized by short duration development cycles that produce demonstrable "interim deliveries" of software which may or may not be fielded to the operational community. The time required to create delivery iteration is dependent on planning, complexity of features, or other influences. Iterations may also be based on a fixed time cycle, with variances in the amount of features developed. The contractor is expected to use continuous integration best practices in developing software solutions.

C.5.9.3.3 The contractor shall perform all the associated activities required to develop, integrate, implement, and sustain the solution. The contractor shall be responsible for overall responsiveness, cost control, adherence to schedules, and technical quality of work.

C.5.9.4 SUBTASK 4 – SYSTEM ANALYSIS

C.5.9.4.1 The contractor shall provide detailed requirement analysis (see Section F, Deliverable #76) on proposed changes to existing applications and proposed new functionality. Each analysis shall address, at a minimum, the following criteria: availability, maintainability, expandability, reliability, and conformance to functional, security, and budgetary requirements. The analysis shall identify the resources, risks, dependencies, and impact associated with the requirement.

The contractor shall:

- Review all Government-proposed requirements entered as Enterprise Change Proposal (ECP) in the Dimensions system. Gather customer technical detail requirements.

- Determine the impact on any internal/external system(s).
- Coordinate meetings with Government leads.
- Provide fully justified Courses of Action (COA) based on current industry-accepted methodologies coupled with innovative solutions.
- Document results and findings, providing recommendations on systems integration and standardization as required. (See Section F Deliverables #77, #78, #79, #80, #82).
- Develop detailed implementation plans.
- Provide real-time visibility mechanism for Government review and feedback for software development projects.
- Utilize existing and proposed future software toolsets to automate existing and future IE.
- Develop a Requirements Specification Document (Deliverable #81) upon project assignment decision.

C.5.9.4.2 The contractor shall ensure the requirements comply with and conform to Army Architecture standards, DOD IA requirements, the DOD Architecture Framework, and the ARNG-approved architecture. The contractor shall not have any direct communication with a Government customer without a TPOC-designated representative being present.

C.5.9.4.3 The contractor shall ensure the analysis activities result in a defined set of functional and technical requirements. By Government direction, these requirements may be transitioned to a development group for implementation. The analysis shall also address standard operating procedures, policies, system interfaces, and service level agreements.

C.5.9.4.4 As part of the requirements management activity, the contractor shall implement a change control process designed to add rigor in managing changes to the existing requirements baseline. Although changes are anticipated they are managed through the change control process designed to minimize requirements scope challenges with a proactive process to assess costs and impacts to proposed requirements changes.

C.5.9.5 SUBTASK 5 – IMA CORE SUSTAINMENT

C.5.9.5.1 SOFTWARE DEVELOPMENT

C.5.9.5.1.1 The contractor shall provide system development and maintenance in support of the National Guard. The contractor shall perform all the IMA-associated activities required to enhance, integrate, implement, and maintain the solution.

C.5.9.5.1.2 The contractor shall provide system sustainment services and development for software applications, database applications, and other solutions, to include all the associated activities required to update/changes, enhance, integrate, implement, and maintain the IMA solutions. The contractor shall update all existing system documentation as required during the course of development and maintenance. The contractor shall be responsible for the preparation of additional systems documentation that may be required by change in system requirements. (Deliverables #21, #24, #27, #28, and #83)

C.5.9.5.1.3 The contractor shall possess an in-depth understanding of the overall system development, system design and functionality requirements to include system of systems interfaces. The contractor shall sustain system baselines and functionality for IMA. The contractor shall sustain functionality of the complete family of software applications, ensuring timely security and products updates and quality releases. The contractor shall be responsible for overall responsiveness, cost control, adherence to schedules, and technical quality of work.

C.5.9.5.2 SIDPERS TRANSITION TO IPPS-A

C.5.9.5.2.1 The contractor shall continue Standard Installation/Division Personnel System (SIDPERS) maintenance until IPPS-A is operational.

C.5.9.5.2.2 The Contractor shall assist in the preparation of plans for the transition of the SIDPERS data to IPPS-A. This will include the backup, archival, and decommissioning / restoration for SIDPERS. The fully executable plans and processes are needed to ensure SIDPERS (system, documentation, source code, test information, etc.) is saved for future use and to restore the system if necessary. The timeline that should be followed for the plan is that backup will be completed within one week, all data will be fully inventoried and archived, and system will be restored within two weeks.

C.5.9.5.2.3 The contractor shall assist in the execution of the SIDPERS transition plan.

C.5.9.5.2.4 The contractor shall evaluate the transition of SIDPERS interfaces to IPPS-A. The contractor shall verify inbound and outbound interfaces associated with SIDPERS to ensure all file layouts, domain names, and valid domain values are documented.

C.5.9.5.3 TAPDB-G SUPPORT

The contractor shall collaborate with the Government to make changes to TAPDB-G reflecting changes created by the implementation of IPPS-A to include regulations, policies, etc. The contractor shall ensure timely updates are made to TAPDB-G to be consistent with IPPS-A and other source systems.

C.5.9.5.4 DATABASES

The contractor shall develop databases (see Section F, Deliverable #83), monitor and sustain the databases and incorporate changes, or updates, to the supporting data models, schemas, and related support software as required. The contractor shall provide continuous improvement in the integration of the information within the database to facilitate data sharing across the application systems. The contractor shall maintain an awareness of the Government data standards and evolve existing databases toward continuing compliance with Government data systems.

C.5.9.6 SUBTASK 6 – SOFTWARE DEPLOYMENT MANAGEMENT

C.5.9.6.1 The contractor shall assist the Government in developing a software deployment roadmap that encompasses the individual detailed project plans. The contractor shall assist the Government in developing an integrated software deployment management solution that ensures simplicity in update installation and system use and reduces the implementation burden on units in the field. The contractor shall ensure its software deployment management practices and processes are complementary to the Government's practices and processes.

C.5.9.6.2 The software detailed project plans shall include tasks associated with fielding updates to the sustained application base. The contractor shall build release packages for each application release that include, but are not limited to, the following content:

a. Software Version Description Document that includes the content of each update and any known limitations.
b. Unique identifiers for each update.
c. Installation instructions and release media.

C.5.9.6.3 Release Manager

C.5.9.6.3.1 The contractor shall package releases (see Section F, deliverable #26) for all applications, check bytes size on UNIX and Windows servers, create notifications emails and/or all states releases emails, Secure File Transfer Protocol (SFTP) releases to key states , upload releases to Guard Knowledge Online (GKO) website, and maintain files on website. Each year old files are to be purged from GKO website. The contractor shall participate in the release planning team and its process, including feature releases with other Government-directed representatives.

C.5.9.6.3.2 The contractor shall create a test plan (see Section F, Deliverable #84). Based on a plan for each release, software releases shall be completed, delivered, and fielded. Most projects will require several iterations culminating in a release to the field. Every release will be tailored to the scope of the project, driving longer or shorter iteration and release schedules as required and directed by the Government.

C.5.9.6.3.3 The contractor is responsible for packaging and releasing to the Government applications developed by another contractor. The contractor will not be responsible for developing and testing the following applications under this task:

	ELECTRA
CAPS-W	Commercial Accounts Payable System-Windows
DMO	Defense MilPay Office
GFEBS	General Funds Enterprise Business System
IPERMS	Interactive Personnel Electric Records Management System
IMAP-W	Integrated Automation Program – Web
ODS	Operational Data Store
RCAS	Reserve Component Automation System

RFMSS	Range Facility Management Support System
RPAM	Retirement Points Accounting Management
WINIATS	Windows Integrated Automated Travel System

C.5.9.7 SUBTASK 7- CONFIGURATION MANAGEMENT

C.5.9.7.1 The contractor shall develop a Configuration Management Plan (CMP) (see Section F, Deliverable #32) and establish and maintain a strict change control process. The Contractor shall manage strict version control on all software source code and related artifacts either acquired or developed per the Government-approved Contractor CMP.

C.5.9.7.2 The contractor shall coordinate with Government personnel on changes to the environment through the change control process outlined in the contractor CMP and in accordance with the Government's configuration management guidance.

C.5.9.7.3 The contractor shall provide QC across products' lifecycle to include unit, integration, regression, and security (STIG, etc.) testing to ensure the delivery of quality DOD-compliant products.

C.5.9.7.4 The contractor shall support the IMA with CM activities, to include preparing CM documentation for enterprise and project artifacts; participating in CM planning; overseeing and participating in library setup and control for all developmental components and products; participating in the identification and marking of baseline product components; working with division, project, and QA management to identify and resolve quality issues; participating in process improvement initiatives; supporting configuration control boards; and developing, documenting, and executing CM policies, processes, and SOPs.

C.5.9.7.5 The contractor shall sustain configuration control and configuration documentation, as well as report configuration status, in accordance with ANSI/EIA Standard 649 (National Consensus Standard for Configuration Management); ISO/IEC Standard 12207-2008, Systems and Software Engineering-Software Life Cycle Processes; IEEE Standard 828:2012, Standard for Software Configuration Management Plans; ISO/IEC Standard 15288-2008, Systems and Software Engineering-System Life Cycle Processes; ISO/IEC/IEEE Standard 15289-2011, Systems and Software Engineering – Content of Life-Cycle information products (documentation); and Military Handbook 61A, Configuration Management Guidance, 7 February 2001.

C.5.9.7.6 The contractor shall support CM of requirements such as software and ECPs in response to security vulnerabilities, directed architecture changes, policy/regulatory changes, legislative changes, interface changes, BPIs, environmental changes.

C.5.9.7.7 The contractor shall use the Government implementation of Serena Dimensions (through a secure remote connection (e.g., CITRIX or .mil)) for CM. The contractor shall maintain the baselines and documentation for all system releases. The contractor shall monitor

and report the installation status of each new release. This will include source code control, baseline management, and documentation control.

C.5.9.8 SUBTASK 8 – TESTING

C.5.9.8.1 PRODUCT TESTING

C.5.9.8.1.1 The contractor shall ensure all products are thoroughly tested prior to delivery to the Government. The Government envisions a user-driven, iterative Software Development Life Cycle (SDLC) that includes frequent engagement of the customer and designated representative testers. The approach shall include use of automated regression testing techniques and utilities included as part of a continuous software integration process. The contractor shall support the Government to identify and correct product testing issues identified throughout the software development process, but especially during integration testing of a releasable set of software features.

C.5.9.8.1.2 The contractor shall conduct tests (e.g., unit, functional, system, interoperability, regression, security, and performance) of software throughout the development lifecycle using industry best practices of continuous integration methods and automated regression testing utilities. The IMA Government test lab is 30% virtualized. Testing materials (scripts, configurations, utilities, tools, plans, and results) shall be maintained under configuration control using identical methods applied to source code (see Section F, deliverable #33).

C.5.9.8.1.3 The contractor shall develop and deliver test procedures, test data, materials, results, and artifacts (see Section F, Deliverable #19) in a format that allows the Government to reproduce the testing procedures and results within their own Secure Testing and Integration Environment (STIE). The Government will provide test data as necessary for the contractor to maintain the application and this test data will be provided during transition-in (see Task 1).

C.5.9.8.1.4 The contractor shall conduct testing related to non-functional requirements, including load, performance, and installation testing.

C.5.9.8.1.5 The contractor shall correct and repair software defects throughout the software development process identified through all testing (including unit, system, functional, security, performance, and load testing) procedures.

C.5.9.8.1.6 The contractor shall conduct inspections and provide analysis of testing results as directed (see Section F, Deliverable #85).

C.5.9.8.1.7 The contractor shall provide facilities and hardware for testing software iterations prior to delivery to the Government.

C.5.9.8.1.8 The contractor shall include the user/customer as part of the iteration tests/demonstrations as required.

C.5.9.8.1.9 The contractor shall collect systems and application performance and load data as part of testing process.

C.5.9.8.1.10 Testing scripts, utilities, test execution, and testing results shall be historically maintained under configuration control for comparison and analysis.

C.5.9.8.2 Integration Testing

The contractor shall support the Government's efforts to conduct integration testing of software deliverables within the Government's STIE.

C.5.9.8.3 Repair of Defects

The contractor shall correct and repair software defects discovered during Government integration testing procedures. Defects include issues found within the software, installation procedures, documentation, or other items relevant to successful testing and deployment of a releasable software delivery.

C.5.9.9 SUBTASK 9 – GOVERNMENT SECURE TESTING & INTEGRATION ENVIRONMENT (STIE)

C.5.9.9.1 The contractor shall deliver source codes, build materials, and related artifacts to the Government (see Section F, deliverable #38). Source code evaluation and scanning, installation kit construction, and testing (functional, security, load, performance, etc.) will be conducted within the Government's Common STIE at IMA.

C.5.9.9.2 The contractor shall support Government efforts to build installation kits, conduct design analysis, and perform security scans within the Government facility. For all deliveries, the contractor shall provide media for all source code, installation kits, documentation (see Section F, Deliverable #36) (including those related to architecture, test design and testing results, and installation procedures), and build procedures and scripts delivered to or maintained for the Government.

C.5.9.9.3 When requested by the Government, the contractor shall provide onsite support configuration management and installation of software into the test environment. The contractor shall ensure that the Government is provided copies of all software and related materials developed under this TO at the end of each release or as requested by the Government (see Section F, deliverable #24 and #27). The contractor shall identify third-party products used to develop, operate, and construct the software applications.

C.5.9.10 SUBTASK 10 – IA SECURITY, RISK REMEDIATION, AND MITIGATION

The contractor shall assist the Government in completing DIACAP activities and supporting documentation.

C.5.9.10.1 The contractor shall assist the Government to complete, review, and submit the System Questionnaire in the Army approved database (currently Certification and Accreditation Database (C&A TdB)). The contractor shall monitor and identify current DIACAP Activity Cycle (Initial, Annual Review, Recertification, and Decommission). The contractor shall ensure accuracy before submission to the Certifying Authority Representative (CAR). If the CAR does not concur with the System Questionnaire, the contractor shall remedy and resubmit.

C.5.9.10.2 The contractor shall provide system documentation/artifacts to include network topology diagram, data flow diagram, and hardware and software to be uploaded in the Certification and Accreditation Tracking Database System (C &A TdB). The contractor shall complete the DIACAP Implementation Plan (DIP).

C.5.9.10.3 The contractor shall work with the Agent of the Certifying Authority (ACA) Team(s) to determine availability and ability of the ACA team to perform the IA assessment.

C.5.9.10.4 The contractor shall ensure an IA strategy describes concisely how a program's IA features comply with applicable Federal, DOD and the ARNG standards, regulations, and requirements. The IA strategy shall briefly describe the system, the program's risk assessment in the face of cyber and physical threats, the acquisition strategy, and the certification and accreditation approach. The Government anticipates that the IA strategy should evolve as a program matures.

C.5.9.10.5 The contractor shall provide input to the Government in support of required POA&M submissions, identifying risks in support of the Government's remediation and mitigation plan of action throughout the POA&M process.

C.5.9.10.6 The contractor shall perform audits of production assets to maintain and ensure compliance. The contractor shall provide guidance and recommendations on implementation of new or updated STIGs and SRRs.

C.5.9.10.7 The contractor shall comply with all applicable Information Assurance Vulnerability Management (IAVM) policies and tools prescribed by DOD and Army policy.

C.5.9.10.8 The contractor shall track and provide quarterly updates to the POA&M items.

C.5.9.10.9 The contractor shall assist the Government in submitting and correcting the CoN (AR 25-1) application required by NETCOM for the applications, systems, networks, and/or information systems. The Contractor shall follow CoN instructions put forth by NETCOM for this requirement.

C.5.9.10.10 The contractor shall provide analysis of vulnerabilities identified during security scans such as DISA STIGs, Retina, Fortify or any future tool. The contractor shall advise the Government on the strategy to remediate the vulnerabilities.

C.5.9.11 SUBTASK 11 – LEGACY COTS/ GOTS SOFTWARE

C.5.9.11.1 COTS SOFTWARE

The contractor shall analyze potential modification to specific COTS products and their corresponding application in order to ensure effective and efficient operations as approved by the Government.

The contractor shall ensure integration and complete compatibility of all current and future infrastructure COTS software with the project baseline. The contractor shall obtain, assess, and test patches, fixes, and upgrades of infrastructure COTS software. The contractor shall assess and test infrastructure COTS software upgrades. The contractor shall update and provide software documentation. The contractor shall develop a strategy and methodology to report and resolve COTS software end-of-life issues to the Government.

C.5.9.11.2 GOTS SOFTWARE

The contractor shall assess, test, and integrate replacement/upgraded GOTS applications into the system architecture(s) and ensure integration and complete compatibility of all current and future GOTS applications. The contractor shall develop a strategy and methodology to report and resolve GOTS application software end-of-life issues to the Government. The Contractor shall update and provide software documentation (see Section F, Deliverable #86). The Contractor shall support the GOTS Software Baseline.

C.5.9.11.3 QUALITY CONTROL

The contractor shall provide a Quality Control Plan (QCP) (see Section F, Deliverable #7) that ensures the technology products, services, and solutions provided are integrated and meet best commercial practices. At a minimum, the QCP shall adhere to ISO for QC requirements, or other comparable standards subject to Government approval. The Contractor shall ensure the technology products, services, and solutions it provides are of high quality and are fully integrated and tested to include hardware, software, security, operating systems, and networks.

The contractor shall plan, develop, document and implement a SQA Program (see Section F, deliverable #22) to ensure that high levels of software quality are attained and all contractual requirements are complied with fully. The contractor's SQA Program shall be applied to, but not limited to, the following: software requirements; software design; software engineering standards, practices and procedures; computer program implementation; software documentation, software testing; software library controls; configuration management; corrective action; and subcontractor control.

C.5.9.11.4 SYSTEMS ARCHITECTURE

The contractor shall ensure any future system architecture is sufficiently sized, maintained, and robust enough to support the timely execution of workload. When implementing upgrades, the contractor shall ensure integration and compatibility with the most current architectural directives. The contractor shall ensure that all design changes are interoperable with the most current and future planned infrastructure and to target all applications in the Installation Processing Node (IPN).

C.5.9.12 SUBTASK 12 – ASSET MANAGEMENT

C.5.9.12.1 The contractor shall develop processes and methodologies to safeguard and maintain full visibility and accountability of all equipment and tools, deployed hardware, software, IT assets, and COTS software license and warranty management information placed under their control.

C.5.9.12.2 The contractor shall track the shipment and receipt of Government property in accordance with FAR Part 45 (Government Property). The contractor shall allow the Government representative unlimited access to all Government equipment and records pertaining to inventory and property accountability. The contractor shall utilize the standard Army Asset Management System, Property Book Unit Supply – Enhanced (PBUS-E). Individuals assigned the task of entering data into PBUS-E shall access military networks and therefore require elevated privileges.

C.5.9.12.3 The contractor shall assist the Government representative with the task of obtaining National Stock Numbers (NSNs) for equipment and properly transfer accountability of the equipment, as directed by the Government. The contractor shall be responsible for safeguarding and maintaining full accountability for all equipment, software, or tools placed under their control.

C.5.9.12.4 The contractor shall store and dispose of Government property in accordance with regulatory guidance, unless otherwise directed by the Government.

C.5.9.13 SUBTASK 13 – ENTERPRISE SERVICE DESK

C.5.9.13.1 The contractor shall provide Level 2 and 3 help desk support to IMA. Emergency Remedy tickets should be resolved within 48 hours of receipt (see Section F, deliverable #54). For example, system application failure represents an emergency. **IMA** receives approximately 15 emergency, 40 urgent, and 110 routine Remedy tickets annually.

C.5.9.13.2 The contractor shall use the ARNG Enterprise Service Desk. This support will identify customer problems and solutions and maintain corrective procedures that are reusable and repeatable across the enterprise. The contractor shall review, modify, and develop standards

and procedures for the problem resolution process. This includes focusing on customer call reduction and the use of root cause analysis.

C.5.9.13.3 The contractor shall acknowledge the receipt and provide an interim status on all trouble tickets received from users within 24 hours of the submittal of the trouble ticket. The contractor shall resolve all trouble tickets within 72 hours of receipt. All business-critical tickets pertaining to designated mission-critical systems shall be resolved within 24 hours of receipt. The contractor shall report daily to the designated Government personnel all trouble tickets open longer than 72 hours.

C.5.9.13.4 The contractor shall monitor both Government and contractor problem resolution processes. The contractor shall measure performance and analyze data to isolate and solve computing, security, and networking problems. The contractor shall provide technical analyses of trouble tickets. The contractor shall identify, report, and correct defective system components discovered through analysis of trouble tickets.

C.5.9.14 SUBTASK 14 –INFORMATION ASSURANCE (IA) REQUIREMENTS

Section C.5.3.12.2.1 and C.5.3.12.2.2 applies to this subtask.

C.5.9.15 SUBTASK 15 – CONDUCT TRAINING

The contractor shall provide an innovative approach(s) to end user training. The contractor shall conduct classes on Enterprise Data Warehouse (EDW) yearly.

Trips	Classes	Locations	Curriculum
1	1-2	East coast	EDW
1	1-2	East coast	SMS-A

C.5.10 TASK 10 – SURGE/SPECIAL PROJECTS

The contractor shall provide surge support for RCAS, DLP, ITII&R, and IMA requirements and systems. Potential areas where surge support may be required include, but are not limited to, RC unit mobilization (Presidential Reserve Call-up through Total Mobilization), support to domestic emergencies that require the extension of RCAS system capabilities in support of RC operational requirements, and RC continuity of operations/disaster recovery. Surge support shall be in addition to TO core sustainment requirements, but inclusive of implementation of approved technology initiatives. While the government reserves the right of final approval, a joint determination will be made by the Government and contractor as to where EVM will be applicable. Generally, the Government will not require EVM to be applied against level of effort (LOE) tasks or firm-fixed price (FFP) activities. Due to the general nature of the Surge/Special

Projects tasks, (short period of performance , Level of Effort), EVM will not be required unless requested by the Government. The contractor shall be prepared to provide support for unanticipated surge support requirements including system, system component, or application failure; systems integration; systems deployment; and training, see deliverables below.

a. Status Report (see Section F, Deliverable #87)
b. Implementation Plan (see Section F, Deliverable #88)
c. Technical Information Package (TIP) (see Section F, Deliverable #89)
d. Installation Manual (see Section F, Deliverable #90)
e. Integration Manual (see Section F, Deliverable #91)
f. Emerging Technology Report (see Section F, Deliverable #92)
g. Systems Improvement Initiatives (see Section F, Deliverable #93)
h. As-Built Drawings (see Section F, Deliverable #94) Project
i. Schedule and Cost Estimate (see Section F, Deliverable #95)

See examples in Section J, Attachment AT.